

(19)



Europäisches Patentamt  
European Patent Office  
Office européen des brevets



(11)

**EP 1 143 656 B1**

(12)

## EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention  
of the grant of the patent:  
**03.11.2004 Bulletin 2004/45**

(51) Int Cl.7: **H04L 9/08**

(21) Application number: **01108600.6**

(22) Date of filing: **05.04.2001**

(54) **Copyright protection system, encryption device, decryption device, and recording medium**

Urheberrechtsschutzsystem, Verschlüsselungsvorrichtung, Entschlüsselungsvorrichtung und  
Aufzeichnungsmedium

Système de protection de droits d'auteur, dispositif de chiffage, dispositif de déchiffage et support  
d'enregistrement

(84) Designated Contracting States:  
**DE FR GB**

• **Sekibe, Tsutomu**  
**Hirakata-shi, Osaka 573-0047 (JP)**

(30) Priority: **06.04.2000 JP 2000105525**

(74) Representative: **Balsters, Robert et al**  
**Novagraaf SA**  
**25, Avenue du Pailly**  
**1220 Les Avanchets - Geneva (CH)**

(43) Date of publication of application:  
**10.10.2001 Bulletin 2001/41**

(73) Proprietor: **MATSUSHITA ELECTRIC INDUSTRIAL**  
**CO., LTD.**  
**Kadoma-shi, Osaka 571-8501 (JP)**

(56) References cited:  
**EP-A- 0 800 312** **EP-A- 0 878 796**  
**EP-A- 0 994 475**

(72) Inventors:

• **Shibata, Osamu**  
**Moriguchi-shi, Osaka 570-0032 (JP)**

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

**EP 1 143 656 B1**

## Description

### BACKGROUND OF THE INVENTION

#### 1. FIELD OF THE INVENTION:

[0001] The present invention relates to a communication system performing cryptographic communication in which digital contents, such as music, images, videos, and games, having a decryption limitation are transferred using a common key which is shared by devices so that the decryption of the digital contents is forbidden when the updating of the decryption limitation is unauthorized. More particularly, the present invention relates to a copyright protection system, an encryption device, a decryption device, and a recording medium for protecting copyrights by associating update information on the decryption limitation with the common key.

#### 2. DESCRIPTION OF THE RELATED ART:

[0002] Recently, the development of digital information compression technologies and the explosive pervasion of communication infrastructures have realized that contents, such as music, images, videos, and games, are distributed in the form of digital information via communication lines to homes.

[0003] The digital information distributed via communication lines is in the form of data which is not stored in any medium. Therefore, the flexibility of distribution service forms is dramatically increased. Distribution services can not only provide digital contents but also limit the use of the contents (e.g., the limited number of uses and the limited period of use). A wide variety of distribution service forms are contemplated.

[0004] The establishment of distribution systems, in which the copyrights of digital contents and the profits of distributors are protected, requires solving how to prevent unauthorized actions, such as fraud possession by communication intercept, eavesdropping, pretending, or the like, and illegal duplications and falsifications of received data stored in a recording medium. Such a solution would be provided by copyright protection technologies, such as an encryption/authentication technique performing the identification of authentic systems, data scramble, and the like.

[0005] There are a variety of conventional copyright protection technologies. A typical technology is a challenge-response type mutual authentication system in which random numbers and response values are exchanged between a data encryption device and a data decryption device so that both devices are mutually authenticated, and data is transferred when the authentication is established.

[0006] The term "decryption limitation" as used herein refers to information on whether contents transferred from an encryption device to a decryption device are allowed to be used (e.g., reproduce to make a sound). For

example, when contents are associated with the number of times the contents can be reproduced, such a number of times is a decryption limitation.

[0007] The term "updating of a decryption limitation" as used herein refers to a rule which is used in updating a decryption limitation. For example, for contents associated with the number of times the contents can be reproduced (e.g., N times), such a number of times is a decryption limitation transferred from an encryption device to a decryption device, and the updating of the decryption limitation means that the number of times is reduced by one.

[0008] The term "update information on a decryption limitation" as used herein refers to a decryption limitation which is updated. For example, for contents associated with the number of times the contents can be reproduced (e.g., N times), the number of times which is a decryption limitation transferred from an encryption device to a decryption device, is updated so that the update information on the decryption limitation is rewritten to "N-1 times".

[0009] A typical cryptographic communication system in which digital contents having a decryption limitation are transferred using the above-described mutual authentication technique, will be described. An encryption device and a decryption device are mutually authenticated. Only when the authentication is established, the decryption limitation is encrypted and then transferred from the encryption device to the decryption device. The decryption device interprets the decryption limitation to determine whether the digital contents can be decrypted, and updates the decryption limitation. The update information on the updated decryption limitation is encrypted and transferred to the encryption device. Thereafter, the contents are encrypted and loaded into the decryption device which in turn decrypts the loaded contents.

[0010] A decryption limitation should be correctly updated. In other words, update information on a decryption limitation decrypted by a decryption device should be received by an authenticated encryption device. If a decryption limitation is not correctly updated, i.e., update information on a decryption limitation decrypted by a decryption device is received by a false encryption device pretending to be an authenticated encryption device, the decryption limitation is not updated by the authenticated encryption device and contents loaded from the authenticated encryption device are decrypted by the decryption device in an unauthorized manner. Therefore, a system is required in which, when update information on a decryption limitation decrypted by a decryption device is received by a false encryption device pretending to be an authenticated encryption device, the decryption device is forbidden to decrypt contents loaded from the authenticated encryption device.

[0011] In the above-described mutual authentication technique, a determination is made only as to whether communicating devices are authenticated. Whether a

decryption limitation is currently updated is not determined. Therefore, an unauthorized action cannot be prevented. If update information on a decryption limitation decrypted by a decryption device is received by a false encryption device pretending to be an authenticated encryption device, the decryption limitation is not updated by the authenticated encryption device, and nevertheless contents loaded from the authenticated encryption device cannot be decrypted by the decryption device in an unauthorized manner.

**[0012]** Reference may be made to EP-A-0878796 which describes an information recording apparatus comprising an encryption section encrypting contents information and also a license condition referred to to limit use of the contents information and a fixed decoding key for decoding the encrypted contents information to generate license information, and a recording section recording the encrypted contents information and the generated license information on a recording medium. An information reproducing apparatus comprises a decoder unit decoding the license information recorded on the recording medium using a second decoding key for decoding the license information and deciding on the basis of the license condition contained in the decoded license information whether the contents information can be used. If it is decided that the contents information can be used, the encrypted contents information recorded on the recording medium is decoded using the first decoding key contained in the decoded license information.

#### SUMMARY OF THE INVENTION

**[0013]** Aspects of the invention are defined in the claims.

**[0014]** In a preferred embodiment, a copyright protection system comprises an encryption device and a decryption device, wherein cryptographic communication is performed between the encryption device and the decryption device using a contents key. The encryption device includes a contents storage section for storing contents, a first contents key generation section for generating the contents key based on a second decryption limitation obtained by updating a first decryption limitation, and a first encryption section for encrypting the contents using the contents key and outputting the encrypted contents. The decryption device includes a second contents key generation section for generating the contents key from the second decryption limitation, and a first decryption section for decrypting the encrypted contents using the contents key generated by the second contents key generation section.

**[0015]** In one embodiment of this invention, the decryption device further includes a decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and a second encryption section for encrypting the second decryption

limitation using a time-varying key, and outputting the first encrypted decryption limitation. The encryption device further includes a second decryption section for decrypting the first encrypted decryption limitation transferred from the second encryption section using the time-varying key to generate the second decryption limitation. The first contents key generation section generates the contents key based on the second decryption limitation generated by the second decryption section.

**[0016]** In one embodiment of this invention, the encryption device further includes a first common key storage section for storing a common key, a decryption limitation storage section for storing the first decryption limitation, a first random number generation section for generating a first random number, a first mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device, a first time-varying key generation section for generating the time-varying key using the first random number and the second random number in response to the authentication by the first mutual authentication section, and a third encryption section for encrypting the first decryption limitation using the time-varying key and outputting the second encrypted decryption limitation. The decryption device further includes a second common key storage section for storing the common key, a second random number generation section for generating the second random number, a second mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and the first random number, a second time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the second mutual authentication section, and a third decryption section for decrypting the second encrypted decryption limitation using the time-varying key.

**[0017]** In one embodiment of this invention, the decryption device further includes a first decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and a second contents key generation section for generating the contents key based on the second decryption limitation updated by the first decryption limitation updating section. The encryption device further includes a second decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with the decryption limitation updating rule in response to the updating of the first decryption limitation by the first decryption limitation updating section. The first contents key generation section generates the contents key based on the second decryption limitation updated by the second decryption limitation updating section.

**[0018]** In one embodiment of this invention, the en-

crypton device further includes a first common key storage section for storing a common key, a decryption limitation storage section for storing the first decryption limitation, a first random number generation section for generating a first random number, a first mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device, a first time-varying key generation section for generating a time-varying key using the first random number and the second random number in response to the authentication by the first mutual authentication section, and a second encryption section for encrypting the first decryption limitation using the time-varying key and outputting an encrypted decryption limitation. The decryption device further includes a second common key storage section for storing the common key, a second random number generation section for generating the second random number, a second mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and the first random number, a second time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the second mutual authentication section, and a second decryption section for decrypting the encrypted decryption limitation using the time-varying key.

**[0019]** In one embodiment of this invention, the second decryption limitation updating section updates the first decryption limitation to the second decryption limitation in advance. The first contents key generation section generates the contents key from the second decryption limitation. The second decryption limitation updating section stores the second decryption limitation in the decryption limitation storage section in response to the start of processing by the first encryption section.

**[0020]** In one embodiment of this invention, the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers and the common key.

**[0021]** In one embodiment of this invention, the first and second contents key generation sections generate the contents key based on the second decryption limitation and the time-varying key.

**[0022]** In one embodiment of this invention, the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device. The first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers and the respective data sequence key.

**[0023]** In one embodiment of this invention, the encryption device and the decryption device further include respective first and second data sequence key

generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device. The first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers, the common key, and the respective data sequence key.

**[0024]** In one embodiment of this invention, the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device. The first and second contents key generation sections generate the contents key based on the second decryption limitation and the respective data sequence key.

**[0025]** In one embodiment of this invention, the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device. The first and second contents key generation section generate the contents key based on the second decryption limitation, the time-varying key, and the respective data sequence key.

**[0026]** In one embodiment of this invention, the first and second mutual authentication sections mutually authenticate the decryption device and the encryption device, respectively, by communication in accordance with a challenge-response type authentication protocol.

**[0027]** According to another embodiment of the present invention, an encryption device for performing cryptographic communication in association with a decryption device using a contents key, comprises a contents storage section for storing contents, a contents key generation section for generating the contents key based on a second decryption limitation obtained by updating a first decryption limitation, and a first encryption section for encrypting the contents using the contents key and outputting the encrypted contents.

**[0028]** In one embodiment of this invention, the encryption device further includes a decryption section for decrypting the first encrypted decryption limitation transferred from the decryption device using the time-varying key to generate the second decryption limitation, and the contents key generation section generates the contents key based on the second decryption limitation generated by the decryption device.

**[0029]** In one embodiment of this invention, the encryption device further includes a common key storage section for storing a common key, a decryption limitation storage section for storing the first decryption limitation, a first random number generation section for generating a first random number, a mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the de-

encryption device, a time-varying key generation section for generating the time-varying key using the first random number and the second random number in response to the authentication by the mutual authentication section, and a second encryption section for encrypting the first decryption limitation using the time-varying key and outputting the second encrypted decryption limitation.

[0030] In one embodiment of this invention, the encryption device further includes a decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule in response to the updating of a decryption limitation by the decryption device. The contents key generation section generates the contents key based on the second decryption limitation obtained by the decryption limitation updating section.

[0031] In one embodiment of this invention, the encryption device further includes a common key storage section for storing a common key, a decryption limitation storage section for storing the first decryption limitation, a first random number generation section for generating a first random number, a mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device, a time-varying key generation section for generating a time-varying key using the first random number and the second random number in response to the authentication by the mutual authentication section, and a second encryption section for encrypting the first decryption limitation using the time-varying key and outputting an encrypted decryption limitation.

[0032] In one embodiment of this invention, the decryption limitation updating section updates the first decryption limitation to the second decryption limitation in advance. The decryption limitation updating section outputs the second decryption limitation to the contents key generation section. The contents key generation section generates the contents key from the second decryption limitation. The decryption limitation updating section stores the second decryption limitation in the decryption limitation storage section in response to the start of processing by the first encryption section.

[0033] In one embodiment of this invention, the time-varying key generation section generates the time-varying key based on the first and second random numbers and the common key.

[0034] In one embodiment of this invention, the contents key generation section generates the contents key based on the second decryption limitation and the time-varying key.

[0035] In one embodiment of this invention, the encryption device further includes a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device, the time-varying key generation sec-

tion generates the time-varying key based on the first and second random numbers and the data sequence key.

[0036] In one embodiment of this invention, the encryption device further includes a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device. The time-varying key generation section generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key.

[0037] In one embodiment of this invention, the encryption device further includes a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device. The contents key generation section generates the contents key based on the second decryption limitation and the data sequence key.

[0038] In one embodiment of this invention, the encryption device further includes a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the encryption device. The contents key generation section generates the contents key based on the second decryption limitation, the time-varying key, and the data sequence key.

[0039] According to another embodiment of the present invention, a decryption device for performing cryptographic communication in association with an encryption device using a contents key, comprises a contents key generation section for generating the contents key from a second decryption limitation, and a first decryption section for decrypting encrypted contents using the contents key generated by the contents key generation section.

[0040] In one embodiment of this invention, the decryption device further includes a decryption limitation updating section for updating a first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and an encryption section for encrypting the second decryption limitation using a time-varying key, and outputting the first encrypted decryption limitation.

[0041] In one embodiment of this invention, the decryption device further includes a common key storage section for storing the common key, a random number generation section for generating the second random number, a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number, a time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section, and a second decryption section for decrypting a first encrypted decryption limitation using the time-varying key.

[0042] In one embodiment of this invention, the de-

crypton device further includes a decryption limitation updating section for updating the first decryption limitation to a second decryption limitation in accordance with a decryption limitation updating rule. A contents key generation section for generating the contents key based on the second decryption limitation updated by the decryption limitation updating section.

[0043] In one embodiment of this invention, the decryption device further includes a second common key storage section for storing the common key, a second random number generation section for generating the second random number, a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number, a time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section, and a second decryption section for decrypting encrypted decryption limitation using the time-varying key.

[0044] In one embodiment of this invention, the time-varying key generation section generates the time-varying key based on the first and second random numbers and the common key.

[0045] In one embodiment of this invention, the contents key generation section generates the contents key based on the second decryption limitation and the time-varying key.

[0046] In one embodiment of this invention, the decryption device further includes a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device. The time-varying key generation section generates the time-varying key based on the first and second random numbers and the data sequence key.

[0047] In one embodiment of this invention, the decryption device further includes a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device. The time-varying key generation section generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key.

[0048] In one embodiment of this invention, the decryption device further includes a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device. The contents key generation section generates the contents key based on the second decryption limitation and the data sequence key.

[0049] In one embodiment of this invention, the decryption device further includes a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from the decryption device. The contents key generation section generates the contents key based on the second de-

crypton limitation, the time-varying key, and the data sequence key.

[0050] According to another embodiment of the present invention, there is provided a recording medium storing a program for use in causing a computer to perform cryptographic communication with an encryption device using a contents key. The program causes the computer to function as a contents key generation section for generating the contents key from a second decryption limitation, and a first decryption section for decrypting encrypted contents using the contents key generated by the contents key generation section.

[0051] In one embodiment of this invention, the program causes the computer to further function as a decryption limitation updating section for updating a first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and an encryption section for encrypting the second decryption limitation using a time-varying key, and outputting a first encrypted decryption limitation.

[0052] In one embodiment of this invention, the program causes the computer to further function as a common key storage section for storing the common key, a random number generation section for generating a second random number, a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number, a time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section, and a second decryption section for decrypting a first encrypted decryption limitation using the time-varying key.

[0053] In one embodiment of this invention, the program causes the computer to further function as a decryption limitation updating section for updating a first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and a contents key generation section for generating the contents key based on the second decryption limitation obtained by the decryption limitation updating section.

[0054] In one embodiment of this invention, the program causes the computer to further function as a second common key storage section for storing the common key, a second random number generation section for generating the second random number, a mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and a first random number, a time-varying key generation section for generating a time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section, and a second decryption section for decrypting encrypted decryption limitation using the time-varying key.

[0055] In one embodiment of this invention, the time-varying key generation section generates the time-var-

ying key based on the first and second random numbers and the common key.

[0056] In one embodiment of this invention, the contents key generation section generates the contents key based on the second decryption limitation and the time-varying key.

[0057] In one embodiment of this invention, the program causes the computer to further function as a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device. The time-varying key generation section generates the time-varying key based on the first and second random numbers and the data sequence key.

[0058] In one embodiment of this invention, the program causes the computer to further function as a sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device. The time-varying key generation section generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key.

[0059] In one embodiment of this invention, the program causes the computer to further function as a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device. The contents key generation section generates the contents key based on the second decryption limitation and the data sequence key.

[0060] In one embodiment of this invention, the program causes the computer to further function as a data sequence key generation section for generating a data sequence key based on a data sequence input to or output from a decryption device. The contents key generation section generates the contents key based on the second decryption limitation, the time-varying key, and the data sequence key.

[0061] Thus, the invention described herein makes possible the advantages of (1) providing a copyright protection system, an encryption device, a decryption device, and a recording medium, in which a decryption limitation is reliably updated and unauthorized decryption of digital contents is prevented, and (2) providing a copyright protection system, an encryption device, a decryption device, and a recording medium, in which, when update information on a decryption limitation updated by a decryption device is received by a false encryption device pretending to be an authenticated encryption device (instead of the authenticated encryption device), contents loaded from the authenticated encryption device cannot be decrypted by the decryption device.

[0062] These and other advantages of the present invention will become apparent to those skilled in the art upon reading and understanding the following detailed description with reference to the accompanying figures.

## BRIEF DESCRIPTION OF THE DRAWINGS

[0063] Figure 1 is a diagram showing a configuration of a system according to Example 1 of the present invention.

[0064] Figure 2 is a flowchart showing processing steps of the system of Example 1.

[0065] Figure 3 is a diagram showing a configuration of a system according to Example 2 of the present invention.

[0066] Figure 4 is a diagram showing a configuration of a system according to Example 3 of the present invention.

[0067] Figure 5 is a diagram showing a configuration of a system according to Example 4 of the present invention.

[0068] Figure 6 is a diagram showing a configuration of a system according to Example 5 of the present invention.

[0069] Figure 7 is a diagram showing a configuration of a system according to Example 6 of the present invention.

[0070] Figure 8 is a diagram showing a configuration of a system according to Example 7 of the present invention.

[0071] Figure 9 is a diagram showing another configuration of the system of Example 7.

## DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0072] Hereinafter, the present invention will be described by way of illustrative examples with reference to the accompanying drawings. In the present invention, a decryption limitation is used to generate a contents key which is used to encrypt digital contents

(Example 1)

[0073] Figure 1 is a diagram showing a configuration of a system according to Example 1 of the present invention, in which cryptographic communication is performed between an encryption device 101 and a decryption device 102.

[0074] The encryption device 101 includes: a common key storage section 103 for storing a common key UK; a decryption limitation storage section 111 for storing a decryption limitation; a contents storage section 121 for storing contents CT; a random number generation section 105 for generating a random number R1; a mutual authentication section 107 for performing mutual authentication with the decryption device 102 using the random number R1, a random number R2 transferred from the decryption device 102, and the common key UK; a time-varying key generation section 109 for generating a time-varying key VK every time the mutual authentication using the random numbers R1 and R2 is performed in the mutual authentication section 107; an

encryption section 113 for encrypting the decryption limitation S1 using the time-varying key VK, and outputting an encrypted decryption limitation S2; a decryption section 115 for decrypting an encrypted decryption limitation S3 transferred from an encryption section 116 of the decryption device 102, using the time-varying key VK, to a decryption limitation S4, and writing the decryption limitation S4 to the decryption limitation storage section 111; a contents key generation section 117 for generating a contents key CK from the decryption limitation S4; and an encryption section 119 for encrypting the contents CT using the contents key CK, and outputting encrypted contents S5.

[0075] The decryption device 102 includes: a common key storage section 104 for storing the common key UK; a random number generation section 106 for generating the random number R2; a mutual authentication section 108 for performing mutual authentication with the encryption device 101 using the random numbers R1 and R2 and the common key UK; a time-varying key generation section 110 for generating the time-varying key VK in response to the mutual authentication in the mutual authentication section 108; a decryption section 114 for decrypting the encrypted decryption limitation S2 using the time-varying key VK; a decryption limitation updating section 112 for updating the decryption limitation S4 based on a decryption limitation updating rule using the decryption limitation S1 decrypted in the decryption section 114; an encryption section 116 for encrypting the decryption limitation S4 using the time-varying key VK, and outputting the encrypted decryption limitation S3; a contents key generation section 118 for generating the contents key CK from the decryption limitation S4; and a decryption section 120 for decrypting the encrypted contents S5 using the contents key CK, and outputting the contents CT.

[0076] The encryption device 101 and the decryption device 102 include the respective common key storage sections 103 and 104 to hold the same common key UK. The same common key UK is stored in the common key storage sections 103 and 104 in advance, or produced in a production process.

[0077] The encryption device 101 includes the decryption limitation storage section 111 for storing the decryption limitation S1 and the contents storage section 121 for storing the contents CT. The common key storage section 103, the decryption limitation storage section 111, and the contents storage section 121 are provided in a protect region which is not accessed directly from the outside of the encryption device 101.

[0078] Figure 2 is a flowchart showing processing steps of the system 100 of Example 1. The processing steps of the system 100 including the encryption device 101 and the decryption device 102 are hereinafter described with reference to Figures 1 and 2.

[0079] The encryption device 101 and the decryption device 102 include the respective random number generation section 105 and 106 which generate the random

numbers R1 and R2 which are independent of each other. The random numbers R1 and R2 are exchanged between the encryption device 101 and the decryption device 102. The decryption device 102 generates a response value V1 using the random number R1 and the common key UK. The encryption device 101 generates a response value V2 using the random number R2 and the common key UK. The response values V1 and V2 are exchanged between the encryption device 101 and the decryption device 102. The mutual authentication sections 107 and 108 compares the response value V1 with the response value V2 to determine whether the other device is authentic. In this manner, a challenge-response type mutual authentication is performed (S201).

[0080] A determination is made whether the authentication is established in the encryption device 101 and the decryption device 102 (S202). If it is determined that the authentication is not established (NO in S202), the process is ended. If it is determined that the authentication is established (YES in S202), the time-varying key generation sections 109 and 110 generate the same time-varying key VK, which is changed at every mutual authentication, from the respective random numbers R1 and R2 (S203). Thereafter, the decryption limitation S1 stored in the decryption limitation storage section 111 of the encryption device 101 is encrypted in the encryption section 113 using the time-varying key VK, and the encrypted decryption limitation S2 is transferred to the decryption device 102 (S204).

[0081] The decryption section 114 decrypts the received decryption limitation S2 using the time-varying key VK (S205). The decryption limitation updating section 112 updates the decryption limitation S1 decrypted in the decryption section 114, in accordance with the decryption limitation updating rule (S206). The encryption section 116 encrypts the updated decryption limitation S4 using the time-varying key VK (S207), and outputs the encrypted decryption limitation S3 to the encryption device 101. The decryption section 115 decrypts the transferred encrypted decryption limitation S3 using the time-varying key VK, and stores the updated decryption limitation S4 in the decryption limitation storage section 111 (S208).

[0082] The contents key generation section 117 generates the contents key CK from the decryption limitation S4 (S209). When the contents CT stored in the contents storage section 121 are transferred from the encryption device 101 to the decryption device 102, the encryption section 119 encrypts the contents CT using the contents key CK (S210). The contents key generation section 118 generates the contents key CK from the decryption limitation S4 (S211). The encryption section 120 in the decryption device 102 decrypts the encrypted contents S5 using the contents key CK (S212).

[0083] In Example 1, contents are transferred from an encryption device to a decryption device after authentication is established at a single time. Alternatively, mu-



tual authentication may be performed every time the transfer of contents between encryption and decryption devices occurs. In Example 1, the time-varying key **VK** is generated using the random numbers **R1** and **R2** which are used in mutual authentication. Alternatively, the time-varying key **VK** may be generated using the response values **V1** and **V2**.

[0084] Different algorithms or the same algorithm may be used to encrypt and decrypt a decryption limitation and contents. An example of an algorithm is DES (Data Encryption Standard).

[0085] Different algorithms or the same algorithm may be used to generate a time-varying key and a contents key. An example of an algorithm is a one-way function, such as SHA (Secure Hash Algorithm).

[0086] In Example 1, for the sake of simplicity, transmission and reception are performed by the mutual authentication sections 107 and 108, the encryption section 113, the decryption section 114, the decryption section 115, the encryption section 116, the encryption section 119, and the decryption section 120. The transmission and reception are typically managed by control sections 122 and 123. The same applies to examples described later.

[0087] As described above, the copyright protection system of Example 1 performs cryptographic communication by associating the copyrighted contents **CT** with update information on a decryption limitation (the decryption limitation **S4**). Therefore, the contents **CT** cannot be decrypted unless the decryption limitation **S1** is updated in an authorized manner.

(Example 2)

[0088] Figure 3 is a diagram showing a copyright protection system 200 according to Example 2 of the present invention. In Figure 2, the same components as those in Figure 1 are indicated by the same reference numerals. The description thereof is thus omitted.

[0089] In the copyright protection system 100, a decryption limitation **S4** updated in a decryption limitation updating section 112 is encrypted/decrypted and then transferred as is in the copyright protection system 100. In the copyright protection system 200, the decryption limitation **S4** is not stored in a decryption limitation storage section 111, but a decryption limitation updating section 223 is provided in an encryption device 201.

[0090] A decryption limitation updating section 212 in a decryption device 202 transfers only a decryption limitation updating instruction **CC** to update a decryption limitation **S1** to the decryption limitation updating section 223. The decryption limitation updating section 223 receives the transferred decryption limitation updating instruction **CC**, updates the decryption limitation **S1**, and stores the updated decryption limitation **S4** in a decryption limitation storage section 211.

[0091] As described above, the copyright protection system 200 does not need to transfer the updated de-

ryption limitation **S4** associated with generation of the contents key **CK** from the decryption device 202 to the encryption device 201. Therefore, the secrecy of the decryption limitation **S4** is increased. Further, an encryption section and a decryption section (e.g., 116 and 115, respectively, in Figure 1) which involve transfer of the updated decryption limitation **S4** can be deleted, thereby making it possible to reduce the size of the system.

(Example 3)

[0092] Figure 4 is a diagram showing a copyright protection system 300 according to Example 3 of the present invention. In Figure 4, the same components as those in Figure 1 are indicated by the same reference numerals. The description thereof is thus omitted.

[0093] In the copyright protection system 200 of Figure 2, the decryption limitation updating section 223 in the encryption device 201 updates the decryption limitation **S1** according to the updating instruction **CC** from the decryption limitation updating section 212. Unlike the copyright protection system 200, in the copyright protection system 300, the decryption limitation updating section 323 updates a decryption limitation **S1** previously stored in a decryption limitation storage section 311 in an encryption device 301. A contents key generation section 117 generates a contents key **CK** using an updated decryption limitation **S4**. The decryption limitation updating section 323 stores the updated decryption limitation **S4** in a decryption limitation storage section 311 in response to an encryption section 319 starting encryption of contents **CT**.

[0094] As described above, in the copyright protection system 300 of Example 3, the decryption limitation **S1** is not updated according to the instruction from a decryption device 302, but the decryption limitation updating section 323 previously updates the decryption limitation **S1** and the contents key generation section 117 generates the contents key **CK**. Therefore, the processing steps can be reduced.

(Example 4)

[0095] Figure 5 is a diagram showing a copyright protection system 400 according to Example 4 of the present invention. In Figure 5, the same components as those in Figure 1 are indicated by the same reference numerals. The description thereof is thus omitted.

[0096] In the copyright protection system 400, time-varying key generation sections 409 and 410 generate a time-varying key **VK** using a common key **UK** in addition to random numbers **R1** and **R2**. For example, the time-varying key **VK** is generated by an exclusive OR of the random numbers **R1** and **R2** and the common key **UK**, and converting the result using a one-way function.

[0097] As described above, according to the copyright protection system 400, the time-varying key **VK** is generated not only by the random numbers **R1** and **R2**

which can be externally monitored, but in association with the secret common key UK. Therefore, the time-varying key VK is difficult to infer, thereby making it possible to improve the secrecy of the time-varying key VK.

(Example 5)

[0098] Figure 6 is a diagram showing a copyright protection system 500 according to Example 5 of the present invention. In Figure 6, the same components as those in Figure 1 are indicated by the same reference numerals. The description thereof is thus omitted.

[0099] In the copyright protection system 500, contents key generation sections 517 and 518 generate a contents key CK using a time-varying key VK in addition to an updated decryption limitation S4. For example, the contents key CK is generated by an exclusive OR of the decryption limitation S4 and the time-varying key VK, and converting the result using a one-way function.

[0100] As described above, according to the copyright protection system 500 of Example 5, the contents key CK is generated not only by the updated decryption limitation S4, but in association with the time-varying key VK which time-sequentially varies in each mutual authentication. Therefore, the cryptographic security of contents can be improved.

(Example 6)

[0101] Figure 7 is a diagram showing a copyright protection system 600 according to Example 6 of the present invention. In Figure 7, the same components as those in Figure 1 are indicated by the same reference numerals. The description thereof is thus omitted.

[0102] In the copyright protection system 600, an encryption device 601 and a decryption device 602 include data sequence key generation sections 625 and 626, respectively, which generate a data sequence key TK1 from all or part of data input to or output from the encryption device 601 and the decryption device 602. In this case, such input or output data include random numbers R1 and R2, response values V1 and V2, encrypted decryption limitations S2 and S3, and encrypted contents S5. The data sequence key TK1 is additionally used to generate a contents key CK in contents key generation sections 617 and 618.

[0103] The data sequence key TK1 may be generated by counting a High or Low level of each input/output data, for example. The time-varying key VK may be generated by an exclusive OR of the random numbers R1 and R2 and the data sequence key TK1, and converting the result using a one-way function. All input/output data are not necessarily used to generate the data sequence key TK1. A part of the input/output data may be used.

[0104] As described above, in the copyright protection system 600, data input to or output from the encryption device 601 and the decryption device 602 are monitored, and the data sequence key TK1 common to both

devices is generated from the input/output data so that the generated data sequence key TK1 is associated with generation of the contents key CK. Therefore, since the same data is input to and output from an encryption device and a decryption device in a cryptographic system, pretending can be prevented.

(Example 7)

[0105] Figure 8 is a diagram showing a configuration of a system 800 in which cryptographic communication is performed between an encryption device 101 and a decryption device 102. Referring to Figure 8, the encryption device 101 and the decryption device 102 are directly connected to each other. In Figure 8, the same components as those in Figure 1 are indicated by the same reference numerals. The description thereof is thus omitted.

[0106] The system 800 includes a contents reproduction device 801 for reproducing contents. The encryption device 101 is attached to the contents reproduction device 801. The contents reproduction device 801 further includes a decryption device 102 described in Example 1 and a reproduction section 802 for reproducing contents decrypted by the decryption device 102.

[0107] As described above, the decryption device 102 described in Example 1 may be included in the contents reproduction device 801. The encryption device 101 described in Example 1 is attached to the contents reproduction device 801. The encryption device 101 attached to the contents reproduction device 801 and the decryption device 102 included in the contents reproduction device 801 performs cryptographic communication as described in Example 1.

[0108] The contents reproduction device 801 may be a cellular telephone, an audio player, or a personal computer. The encryption device 101 may be a memory card. The encryption device 101 may be any of the encryption devices 201 through 601 described in Examples 2 through 6. The decryption device 102 may be any of the decryption devices 202 through 602 described in Examples 2 through 6.

[0109] The decryption device 102 may be operated in accordance with a program for operating the decryption device described in any of Examples 1 through 6, read from a recording medium 803 in which the program is recorded. The recording medium 803 may be a CD-ROM.

[0110] Figure 9 is a diagram showing another configuration of the system 800 in which cryptographic communication is performed between the encryption device 101 and the decryption device 102. Referring to Figure 9, the encryption device 101 and the decryption device 102 are directly connected to each other via an electric communication line. In Figure 9, the same components as those in Figures 1 and 8 are indicated by the same reference numerals. The description thereof is thus omitted.

[0111] Referring to Figure 9, the system 900 includes a contents reproduction device 801 for reproducing contents, and an electric communication line 903 connecting the contents reproduction device 801 and a server 901. The contents reproduction device 801 includes a decryption device 102 described in Example 1 and a reproduction section 802 for reproducing contents decrypted by the decryption device 102. An encryption device 101 described in Example 1 is attached to the server 901.

[0112] In this manner, the contents reproduction device 801 for reproducing contents and the server 901 are connected to each other via the electric communication line 903. The encryption device 101 is attached to the server 901. The encryption device 101 attached to the server 901 and the decryption device 102 included in the contents reproduction device 801 perform cryptographic communication via the electric communication line 903.

[0113] The electric communication line 903 may be the Internet or a local area network (LAN).

[0114] Similar to the example of Figure 8, the contents reproduction device 801 may be a cellular telephone, an audio player, or a personal computer. The encryption device 101 may be a memory card. The encryption device 101 may be any of the encryption devices 201 through 601 described in Examples 2 through 6. The decryption device 102 may be any of the decryption devices 202 through 602 described in Examples 2 through 6.

[0115] Similar to the example of Figure 8, the decryption device 102 may be operated in accordance with a program for operating the decryption device described in any of Examples 1 through 6, read from a recording medium 803 in which the program is recorded. The recording medium 803 may be a CD-ROM.

[0116] In Figure 9, the encryption device 101 and the decryption device 102 are connected to each other via the electric communication line 903. This invention is not limited to this. The encryption device 101 and the decryption device 102 may be connected to each other via a wireless communication line.

[0117] As described above, according to the present invention, a copyright protection system in which a decryption limitation is reliably updated and unauthorized decryption of digital contents is prevented, an encryption device, a decryption device, and a recording medium, can be provided.

[0118] Further, according to the present invention, a copyright protection system, an encryption device, a decryption device, and a recording medium can be provided, in which, when update information on a decryption limitation updated by a decryption device is received by a false encryption device pretending to be an authenticated encryption device (instead of the authenticated encryption device), advantageously contents loaded from the authenticated encryption device cannot be decrypted by the decryption device.

[0119] Further, according to the present invention, a copyright protection system, an encryption device, a decryption device, and a recording medium can be provided, in which cryptographic communication is performed by associating copyrighted contents with update information on a decryption limitation and, therefore, advantageously the contents cannot be decrypted unless the decryption limitation is updated in an authorized manner.

[0120] Further, according to the present invention, a copyright protection system, an encryption device, a decryption device, and a recording medium can be provided, in which updated decryption limitation associated with generation of a contents key does not need to be transferred from a decryption device to an encryption device and therefore, advantageously the secrecy of the decryption limitation is increased, and further, an encryption section and a decryption section which involve transfer of the updated decryption limitation can be deleted, thereby advantageously making it possible to reduce the size of the system.

[0121] Further, according to the present invention, a copyright protection system, an encryption device, a decryption device, and a recording medium can be provided, in which a decryption limitation is not updated according to an instruction from a decryption device, but rather a decryption limitation updating section previously updates the decryption limitation and a contents key generation section generates the contents key and, therefore, advantageously the processing steps can be reduced.

[0122] Further, according to the present invention, a copyright protection system, an encryption device, a decryption device, and a recording medium can be provided, in which a time-varying key is generated not only by random numbers which can be externally monitored, but also in association with a secret common key and, therefore, the time-varying key is difficult to infer, thereby advantageously making it possible to improve the secrecy of the time-varying key.

[0123] Further, according to the present invention, a copyright protection system, an encryption device, a decryption device, and a recording medium can be provided, in which data input to or output from an encryption device and a decryption device are monitored, and a data sequence key common to both devices is generated from the input/output data so that the generated data sequence key is associated with generation of a contents key and, therefore, pretending can be advantageously prevented.

[0124] Various other modifications will be apparent to and can be readily made by those skilled in the art without departing from the scope of this invention.

## Claims

1. A copyright protection system comprising:

- an encryption device (101) and a decryption device (102), wherein cryptographic communication is performed between the encryption device and the decryption device using a contents key,
- wherein the encryption device includes
- a contents storage section (121) for storing contents,
  - a first contents key generation section (117) for generating the contents key based on a second decryption limitation obtained by updating a first decryption limitation in accordance with a decryption limitation updating rule, and
  - a first encryption section (119) for encrypting the contents using the contents key and outputting the encrypted contents, and
- wherein the decryption device includes
- a second contents key generation section (118) for generating the contents key from the second decryption limitation, and
  - a first decryption section (120) for decrypting the encrypted contents using the contents key generated by the second contents key generation section.
2. A copyright protection system according to claim 1, wherein the decryption device further includes
- a decryption limitation updating section (112) for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and
  - a second encryption section (116) for encrypting the second decryption limitation using a time-varying key, and outputting the first encrypted decryption limitation,
- wherein the encryption device further includes a second decryption section (115) for decrypting the first encrypted decryption limitation transferred from the second encryption section using the time-varying key to generate the second decryption limitation,
- wherein the first contents key generation section (117) generates the contents key based on the second decryption limitation generated by the second decryption section.
3. A copyright protection system according to claim 2, wherein the encryption device further includes
- a decryption limitation storage section (111) for storing the first decryption limitation,
  - a first random number generation section (105) for generating a first random number,
  - a first mutual authentication section (107) for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device,
- a first time-varying key generation section (109) for generating the time-varying key using the first random number and the second random number in response to the authentication by the first mutual authentication section, and
  - a third encryption section (113) for encrypting the first decryption limitation using the time-varying key and outputting the second encrypted decryption limitation, and
- wherein the decryption device further includes
- a second random number generation section (106) for generating the second random number,
  - a second mutual authentication section (108) for performing mutual authentication in association with the encryption device using the second random number and the first random number,
  - a second time-varying key generation section (110) for generating the time-varying key using the second random number and the first random number in response to the authentication by the second mutual authentication section, and
  - a third decryption section (114) for decrypting the second encrypted decryption limitation using the time-varying key.
4. A copyright protection system according to claim 1, wherein the decryption device further includes a first decryption limitation updating section (212) for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule, and
- a second contents key generation section (118) for generating the contents key based on the second decryption limitation updated by the first decryption limitation updating section,
- wherein the encryption device further includes a second decryption limitation updating section (223) for updating the first decryption limitation to the second decryption limitation in accordance with the decryption limitation updating rule in response to the updating of the first decryption limitation by the first decryption limitation updating section,
- the first contents key generation section (117) generates the contents key based on the second decryption limitation updated by the second decryption limitation updating section.
5. A copyright protection system according to claim 4, wherein the encryption device further includes
- a decryption limitation storage section (211) for storing the first decryption limitation,
  - a first random number generation section (105) for generating a first random number,
  - a first mutual authentication section (107) for performing mutual authentication in association with the decryption device using the first random

- number, and a second random number transferred from the decryption device,
- a first time-varying key generation section (109) for generating a time-varying key using the first random number and the second random number in response to the authentication by the first mutual authentication section, and
  - a second encryption section (113) for encrypting the first decryption limitation using the time-varying key and outputting an encrypted decryption limitation, and
  - wherein the decryption device further includes
    - a second random number generation section (106) for generating the second random number,
    - a second mutual authentication section (108) for performing mutual authentication in association with the encryption device using the second random number and the first random number,
    - a second time-varying key generation section (110) for generating the time-varying key using the second random number and the first random number in response to the authentication by the second mutual authentication section, and
    - a second decryption section (114) for decrypting the encrypted decryption limitation using the time-varying key.
6. A copyright protection system according to claim 1, wherein the encryption device further includes a second decryption limitation updating section (323) for updating the first decryption limitation to the second decryption limitation independently of updating by the first decryption limitation section,
    - the first contents key generation section (117) generates the contents key from the second decryption limitation updated by the second decryption limitation updating section (323), and
    - the second decryption limitation updating section (323) stores the second decryption limitation in the decryption limitation storage section in response to the start of processing by the first encryption section.
  7. A copyright protection system according to claim 3, wherein the encryption device further includes a first common key storage section (103) for storing a common key, the decryption device further includes a second common key storage section (104) for storing the common key, and the first and second time-varying key generation sections (109,110) generate the time-varying key based on the first and second random numbers and the common key.
  8. A copyright protection system according to claim 3, wherein the first and second contents key generation sections (117,118) generate the contents key based on the second decryption limitation and the time-varying key.
  9. A copyright protection system according to claim 3, wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections (625,626) for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device, and
    - wherein the first and second time-varying key generation sections (609,610) generate the time-varying key based on the first and second random numbers and the respective data sequence key.
  10. A copyright protection system according to claim 3, wherein the encryption device further includes a first common key storage section (103) for storing a common key, the decryption device further includes a second common key storage section (104) for storing the common key, and the encryption device and the decryption device further include respective first and second data sequence key generation sections (625,626) for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device, and
    - wherein the first and second time-varying key generation sections (609,610) generate the time-varying key based on the first and second random numbers, the common key, and the respective data sequence key.
  11. A copyright protection system according to claim 3, wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections (625,626) for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device, and
    - wherein the first and second contents key generation sections (617,618) generate the contents key based on the second decryption limitation and the respective data sequence key.
  12. A copyright protection system according to claim 3, wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections (625,626) for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device, and wherein the first and second contents key generation section (617,618) generate the contents key based on the second decryption limitation, the time-varying key, and the respective data sequence key.
  13. A copyright protection system according to claim 3, wherein the first and second mutual authentication

sections (107,108) mutually authenticate the decryption device and the encryption device, respectively, by communication in accordance with a challenge-response type authentication protocol.

14. An encryption device for performing cryptographic communication in association with a decryption device using a contents key, comprising:

a contents storage section (121) for storing contents;  
a contents key generation section (117) for generating the contents key based on a second decryption limitation received by the encryption device from the decryption device obtained by updating a first decryption limitation received from the encryption device in accordance with a decryption limitation updating rule; and  
a first encryption section (119) for encrypting the contents using the contents key and outputting the encrypted contents.

15. An encryption device according to claim 14, further including a decryption section (115) for decrypting the first encrypted decryption limitation transferred from the decryption device using the time-varying key to generate the second decryption limitation, and

the contents key generation section (117) generates the contents key based on the second decryption limitation generated by the decryption device.

16. An encryption device according to claim 15, further including

a common key storage section (103) for storing a common key,

a decryption limitation storage section (111) for storing the first decryption limitation,

a first random number generation section (105) for generating a first random number,

a mutual authentication section (107) for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device,

a time-varying key generation section (109) for generating the time-varying key using the first random number and the second random number in response to the authentication by the mutual authentication section, and

a second encryption section (113) for encrypting the first decryption limitation using the time-varying key and outputting the second encrypted decryption limitation.

17. An encryption device according to claim 14, further including a decryption limitation updating section

(223) for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule in response to the updating of a decryption limitation by the decryption device,

wherein the contents key generation section (117) generates the contents key based on the second decryption limitation obtained by the decryption limitation updating section.

18. An encryption device according to claim 17, further including

a common key storage section (103) for storing a common key,

a decryption limitation storage section (111) for storing the first decryption limitation,

a first random number generation section (105) for generating a first random number,

a mutual authentication section (107) for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device,

a time-varying key generation section (109) for generating a time-varying key using the first random number and the second random number in response to the authentication by the mutual authentication section, and

a second encryption section (113) for encrypting the first decryption limitation using the time-varying key and outputting an encrypted decryption limitation.

19. An encryption device according to claim 14, further including a decryption limitation updating section (323) for updating the first decryption limitation to the second decryption limitation independently of updating in a decryption device;

the decryption limitation updating section (323) outputs the second decryption limitation to the contents key generation section;

the contents key generation section (117) generates the contents key from the second decryption limitation generated by the decryption limitation updating section; and

the decryption limitation updating section (323) stores the second decryption limitation in the decryption limitation storage section in response to the start of processing by the first encryption section.

20. An encryption device according to claim 16, wherein the time-varying key generation section (109) generates the time-varying key based on the first and second random numbers and the common key.

21. An encryption device according to claim 16, wherein the contents key generation section (117) gener-

ates the contents key based on the second decryption limitation and the time-varying key.

22. An encryption device according to claim 16, further including a data sequence key generation section (625) for generating a data sequence key based on a data sequence input to or output from the encryption device, the time-varying key generation section (609) generates the time-varying key based on the first and second random numbers and the data sequence key. 5
23. An encryption device according to claim 16, further including a data sequence key generation section (625) for generating a data sequence key based on a data sequence input to or output from the encryption device, wherein the time-varying key generation section (609) generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key. 10 15 20
24. An encryption device according to claim 16, further including a data sequence key generation section (625) for generating a data sequence key based on a data sequence input to or output from the encryption device, wherein the contents key generation section (617) generates the contents key based on the second decryption limitation and the data sequence key. 25 30
25. An encryption device according to claim 16, further including a data sequence key generation section (625) for generating a data sequence key based on a data sequence input to or output from the encryption device, wherein the contents key generation section (617) generates the contents key based on the second decryption limitation, the time-varying key, and the data sequence key. 35 40
26. A decryption device for performing cryptographic communication in association with an encryption device using a contents key, comprising: 45
  - a decryption limitation updating section (112) for receiving a first decryption limitation and for updating the first decryption limitation to generate a second decryption limitation in accordance with a decryption limitation updating rule; 50
  - a contents key generation section (118) for generating the contents key from the second decryption limitation; and
  - a first decryption section (120) for decrypting encrypted contents using the contents key generated by the contents key generation section. 55

27. A decryption device according to claim 26, further including
  - an encryption section (116) for encrypting the second decryption limitation using a time-varying key, and outputting the first encrypted decryption limitation.
28. A decryption device according to claim 27, further including
  - a common key storage section (104) for storing the common key,
  - a random number generation section (106) for generating the second random number,
  - a mutual authentication section (108) for performing mutual authentication in association with the encryption device using the second random number and a first random number,
  - a time-varying key generation section (110) for generating the time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section, and
  - a second decryption section (114) for decrypting a first encrypted decryption limitation using the time-varying key.
29. A decryption device according to claim 26, wherein a contents key generation section (118) for generating the contents key based on the second decryption limitation updated by the decryption limitation updating section.
30. A decryption device according to claim 29, further including
  - a second common key storage section (104) for storing the common key,
  - a second random number generation section (106) for generating the second random number,
  - a mutual authentication section (108) for performing mutual authentication in association with the encryption device using the second random number and a first random number,
  - a time-varying key generation section (110) for generating the time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section, and
  - a second decryption section (114) for decrypting encrypted decryption limitation using the time-varying key.
31. A decryption device according to claim 28, wherein the time-varying key generation section (110) generates the time-varying key based on the first and second random numbers and the common key.
32. A decryption device according to claim 28, wherein the contents key generation section (118) gener-

ates the contents key based on the second decryption limitation and the time-varying key.

33. A decryption device according to claim 28, further including a data sequence key generation section (626) for generating a data sequence key based on a data sequence input to or output from the decryption device,

wherein the time-varying key generation section (610) generates the time-varying key based on the first and second random numbers and the data sequence key.

34. A decryption device according to claim 28, further including a data sequence key generation section (626) for generating a data sequence key based on a data sequence input to or output from the decryption device,

wherein the time-varying key generation section (610) generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key.

35. A decryption device according to claim 28, further including a data sequence key generation section (626) for generating a data sequence key based on a data sequence input to or output from the decryption device,

wherein the contents key generation section (618) generates the contents key based on the second decryption limitation and the data sequence key.

36. A decryption device according to claim 28, further including a data sequence key generation section (626) for generating a data sequence key based on a data sequence input to or output from the decryption device,

wherein the contents key generation section (618) generates the contents key based on the second decryption limitation, the time-varying key, and the data sequence key.

37. A recording medium storing a program for use in causing a computer to perform cryptographic communication with an encryption device using a contents key, wherein:

the program causes the computer to function as:

a decryption limitation updating section (112) for receiving a first decryption limitation and for updating the first decryption limitation to generate a second decryption limitation in accordance with a decryption limitation updating rule; a contents key generation section (118) for generating the contents key from the second decryption limitation; and

a first decryption section (120) for decrypting encrypted contents using the contents key generated by the contents key generation section.

38. A recording medium according to claim 37, wherein the program causes the computer to further function as:

an encryption section (116) for encrypting the second decryption limitation using a time-varying key, and outputting a first encrypted decryption limitation.

39. A recording medium according to claim 38, wherein the program causes the computer to further function as:

a common key storage section (104) for storing the common key;

a random number generation section (106) for generating a second random number;

a mutual authentication section (108) for performing mutual authentication in association with the encryption device using the second random number and a first random number;

a time-varying key generation section (110) for generating the time-varying key using the second random number and the first random number in response to the authentication by the mutual authentication section; and

a second decryption section (114) for decrypting a first encrypted decryption limitation using the time-varying key.

40. A recording medium according to claim 37, wherein:

the program causes the computer to further function as a contents key generation section (118) for generating the contents key based on the second decryption limitation obtained by the decryption limitation updating section.

41. A recording medium according to claim 40, wherein the program causes the computer to further function as:

a second common key storage section (104) for storing the common key;

a second random number generation section (106) for generating the second random number;

a mutual authentication section (108) for performing mutual authentication in association with the encryption device using the second random number and a first random number;

a time-varying key generation section (110) for generating a time-varying key using the second random number and the first random number



in response to the authentication by the mutual authentication section; and  
a second decryption section (114) for decrypting encrypted decryption limitation using the time-varying key.

42. A recording medium according to claim 39, wherein the time-varying key generation section (110) generates the time-varying key based on the first and second random numbers and the common key.

43. A recording medium according to claim 39, wherein the contents key generation section (118) generates the contents key based on the second decryption limitation and the time-varying key.

44. A recording medium according to claim 39, wherein:

the program causes the computer to further function as a data sequence key generation section (626) for generating a data sequence key based on a data sequence input to or output from a decryption device; and  
the time-varying key generation section (610) generates the time-varying key based on the first and second random numbers and the data sequence key.

45. A recording medium according to claim 39, wherein:

the program causes the computer to further function as a sequence key generation section (626) for generating a data sequence key based on a data sequence input to or output from a decryption device; and  
the time-varying key generation section (610) generates the time-varying key based on the first and second random numbers, the common key, and the data sequence key.

46. A recording medium according to claim 39, wherein:

the program causes the computer to further function as a data sequence key generation section (626) for generating a data sequence key based on a data sequence input to or output from a decryption device; and  
the contents key generation section (618) generates the contents key based on the second decryption limitation and the data sequence key.

47. A recording medium according to claim 39, wherein:

the program causes the computer to further function as a data sequence key generation section (626) for generating a data sequence key based on a data sequence input to or output

from a decryption device; and  
the contents key generation section (618) generates the contents key based on the second decryption limitation, the time-varying key, and the data sequence key.

## Patentansprüche

1. Urheberrecht-Schutzsystem, das umfasst:

eine Verschlüsselungsvorrichtung (101) und eine Entschlüsselungsvorrichtung (102), wobei zwischen der Verschlüsselungsvorrichtung und der Entschlüsselungsvorrichtung unter Verwendung eines Inhaberschlüssels eine verschlüsselte Kommunikation ausgeführt wird,

wobei die Verschlüsselungsvorrichtung umfasst:

einen Inhaberspeicherabschnitt (121) zum Speichern von Inhalten,  
einen ersten Inhaberschlüssel-Erzeugungsabschnitt (117) zum Erzeugen des Inhaberschlüssels anhand einer zweiten Entschlüsselungsbeschränkung, die durch Aktualisieren einer ersten Entschlüsselungsbeschränkung in Übereinstimmung mit einer Entschlüsselungsbeschränkungs-Aktualisierungsregel erhalten wird, und  
einen ersten Verschlüsselungsabschnitt (119) zum Verschlüsseln der Inhalte unter Verwendung des Inhaberschlüssels und zum Ausgeben der verschlüsselten Inhalte, und

wobei die Entschlüsselungsvorrichtung umfasst:

einen zweiten Inhaberschlüssel-Erzeugungsabschnitt (118) zum Erzeugen des Inhaberschlüssels aus der zweiten Entschlüsselungsbeschränkung und  
einen ersten Entschlüsselungsabschnitt (120) zum Entschlüsseln der verschlüsselten Inhalte unter Verwendung des Inhaberschlüssels, der durch den zweiten Inhaberschlüssel-Erzeugungsabschnitt erzeugt wird.

2. Urheberrecht-Schutzsystem nach Anspruch 1, bei dem die Entschlüsselungsvorrichtung ferner umfasst:

einen Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt (112) zum Aktualisieren der ersten Entschlüsselungsbeschränkung auf die zweite Entschlüsselungsbeschränkung in Übereinstimmung mit einer Entschlüsselungs-

beschränkungs-Aktualisierungsregel und einen zweiten Verschlüsselungsabschnitt (116) zum Verschlüsseln der zweiten Entschlüsselungsbeschränkung unter Verwendung eines zeitlich veränderlichen Schlüssels und zum Ausgeben der ersten verschlüsselten Entschlüsselungsbeschränkung,

wobei die Verschlüsselungsvorrichtung ferner einen zweiten Entschlüsselungsabschnitt (115) zum Entschlüsseln der ersten verschlüsselten Entschlüsselungsbeschränkung, die von dem zweiten Verschlüsselungsabschnitt unter Verwendung des zeitlich veränderlichen Schlüssels übertragen wird, um die zweite Entschlüsselungsbeschränkung zu erzeugen, umfasst und

wobei der erste Inhaltsschlüssel-Erzeugungsabschnitt (117) den Inhaltsschlüssel auf der Grundlage der zweiten Entschlüsselungsbeschränkung erzeugt, die durch den zweiten Entschlüsselungsabschnitt erzeugt wird.

3. Urheberrecht-Schutzsystem nach Anspruch 2, bei dem die Verschlüsselungsvorrichtung ferner umfasst:

einen Entschlüsselungsbeschränkungs-Speicherabschnitt (111) zum Speichern der ersten Entschlüsselungsbeschränkung, einen ersten Zufallszahl-Erzeugungsabschnitt (105) zum Erzeugen einer ersten Zufallszahl, einen ersten Abschnitt (107) zur gegenseitigen Authentifizierung, um eine gegenseitige Authentifizierung in Verbindung mit der Entschlüsselungsvorrichtung unter Verwendung der ersten Zufallszahl und einer von der Entschlüsselungsvorrichtung übertragenen zweiten Zufallszahl auszuführen, einen ersten Abschnitt (109) zum Erzeugen eines zeitlich veränderlichen Schlüssels, um den zeitlich veränderlichen Schlüssel unter Verwendung der ersten Zufallszahl und der zweiten Zufallszahl in Reaktion auf die Authentifizierung durch den ersten Abschnitt zur gegenseitigen Authentifizierung zu erzeugen, und einen dritten Verschlüsselungsabschnitt (113) zum Verschlüsseln der ersten Entschlüsselungsbeschränkung unter Verwendung des zeitlich veränderlichen Schlüssels und zum Ausgeben der zweiten verschlüsselten Entschlüsselungsbeschränkung und

wobei die Entschlüsselungsvorrichtung ferner umfasst:

einen zweiten Zufallszahl-Erzeugungsabschnitt (106) zum Erzeugen der zweiten Zufallszahl,

einen zweiten Abschnitt (108) zur gegenseitigen Authentifizierung, um eine gegenseitige Authentifizierung in Verbindung mit der Verschlüsselungsvorrichtung unter Verwendung der zweiten Zufallszahl und der ersten Zufallszahl auszuführen,

einen zweiten Abschnitt (110) zur Erzeugung eines zeitlich veränderlichen Schlüssels, um den zeitlich veränderlichen Schlüssel unter Verwendung der zweiten Zufallszahl und der ersten Zufallszahl in Reaktion auf die Authentifizierung durch den zweiten Abschnitt zur gegenseitigen Authentifizierung zu erzeugen, und einen dritten Entschlüsselungsabschnitt (114) zum Entschlüsseln der zweiten verschlüsselten Entschlüsselungsbeschränkung unter Verwendung des zeitlich veränderlichen Schlüssels.

4. Urheberrecht-Schutzsystem nach Anspruch 1, bei dem die Entschlüsselungsvorrichtung ferner umfasst: einen ersten Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt (212) zum Aktualisieren der ersten Entschlüsselungsbeschränkung auf die zweite Entschlüsselungsbeschränkung in Übereinstimmung mit einer Entschlüsselungsbeschränkungs-Aktualisierungsregel und

einen zweiten Inhaltsschlüssel-Erzeugungsabschnitt (118) zum Erzeugen des Inhaltsschlüssels anhand der zweiten Entschlüsselungsbeschränkung, die durch den ersten Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt aktualisiert wurde,

wobei die Entschlüsselungsvorrichtung ferner einen zweiten Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt (223) zum Aktualisieren der ersten Entschlüsselungsbeschränkung auf die zweite Entschlüsselungsbeschränkung in Übereinstimmung mit der Entschlüsselungsbeschränkungs-Aktualisierungsregel in Reaktion auf die Aktualisierung der ersten Entschlüsselungsbeschränkung durch den ersten Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt umfasst,

wobei der erste Inhaltsschlüssel-Erzeugungsabschnitt (117) den Inhaltsschlüssel auf der Grundlage der zweiten Entschlüsselungsbeschränkung, die durch den zweiten Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt erzeugt wurde, erzeugt.

5. Urheberrecht-Schutzsystem nach Anspruch 4, bei dem die Verschlüsselungsvorrichtung ferner umfasst:

einen Entschlüsselungsbeschränkungs-Speicherabschnitt (211) zum Speichern der ersten Entschlüsselungsbeschränkung, einen ersten Zufallszahl-Erzeugungsabschnitt

(105) zum Erzeugen einer ersten Zufallszahl, einen ersten Abschnitt (107) zur gegenseitigen Authentifizierung, um eine gegenseitige Authentifizierung in Verbindung mit der Entschlüsselungsvorrichtung unter Verwendung der ersten Zufallszahl und einer von der Entschlüsselungsvorrichtung übertragenen zweiten Zufallszahl auszuführen, einen ersten Abschnitt (109) zur Erzeugung eines zeitlich veränderlichen Schlüssels, um einen zeitlich veränderlichen Schlüssel unter Verwendung der ersten Zufallszahl und der zweiten Zufallszahl in Reaktion auf die Authentifizierung durch den ersten Abschnitt zur gegenseitigen Authentifizierung zu erzeugen, und einen zweiten Verschlüsselungsabschnitt (113) zum Verschlüsseln der ersten Entschlüsselungsbeschränkung unter Verwendung des zeitlich veränderlichen Schlüssels und zum Ausgeben einer verschlüsselten Entschlüsselungsbeschränkung, und

wobei die Entschlüsselungsvorrichtung ferner umfasst:

einen zweiten Zufallszahl-Erzeugungsabschnitt (106) zum Erzeugen der zweiten Zufallszahl, einen zweiten Abschnitt (108) zur gegenseitigen Authentifizierung, um eine gegenseitige Authentifizierung in Verbindung mit der Verschlüsselungsvorrichtung unter Verwendung der zweiten Zufallszahl und der ersten Zufallszahl auszuführen, einen zweiten Abschnitt (110) zum Erzeugen eines zeitlich veränderlichen Schlüssels, um den zeitlich veränderlichen Schlüssel unter Verwendung der zweiten Zufallszahl und der ersten Zufallszahl in Reaktion auf die Authentifizierung durch den zweiten Abschnitt zur gegenseitigen Authentifizierung zu erzeugen, und einen zweiten Entschlüsselungsabschnitt (114) zum Entschlüsseln der verschlüsselten Entschlüsselungsbeschränkung unter Verwendung des zeitlich veränderlichen Schlüssels.

6. Urheberrecht-Schutzsystem nach Anspruch 1, bei dem die Verschlüsselungsvorrichtung ferner einen zweiten Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt (323) zum Aktualisieren der ersten Entschlüsselungsbeschränkung auf die zweite Entschlüsselungsbeschränkung unabhängig von der Aktualisierung durch den ersten Entschlüsselungsbeschränkungsabschnitt umfasst,

der erste Inhaltsschlüssel-Erzeugungsabschnitt (117) den Inhaltsschlüssel aus der zweiten Entschlüsselungsbeschränkung, die durch den zweiten Entschlüsselungsbeschränkungs-Aktuali-

sierungsabschnitt (323) aktualisiert wird, erzeugt und

der zweite Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt (323) die zweite Entschlüsselungsbeschränkung in dem Entschlüsselungsbeschränkungs-Speicherabschnitt in Reaktion auf den Beginn der Verarbeitung durch den ersten Entschlüsselungsabschnitt speichert.

7. Urheberrecht-Schutzsystem nach Anspruch 3, bei dem die Verschlüsselungsvorrichtung ferner einen ersten Abschnitt (103) zum Speichern eines gemeinsamen Schlüssels, um einen gemeinsamen Schlüssel zu speichern, umfasst, die Entschlüsselungsvorrichtung ferner einen zweiten Abschnitt (104) zum Speichern des gemeinsamen Schlüssels, um den gemeinsamen Schlüssel zu speichern, umfasst und der erste und der zweite Abschnitt (109, 110) zur Erzeugung des zeitlich veränderlichen Schlüssels den zeitlich veränderlichen Schlüssel auf der Grundlage der ersten und der zweiten Zufallszahl sowie des gemeinsamen Schlüssels erzeugen.

8. Urheberrecht-Schutzsystem nach Anspruch 3, bei dem der erste und der zweite Inhaltsschlüssel-Erzeugungsabschnitt (117, 118) den Inhaltsschlüssel anhand der zweiten Entschlüsselungsbeschränkung und des zeitlich veränderlichen Schlüssels erzeugen.

9. Urheberrecht-Schutzsystem nach Anspruch 3, bei dem die Verschlüsselungsvorrichtung und die Entschlüsselungsvorrichtung ferner einen ersten bzw. einen zweiten Datensequenzschlüssel-Erzeugungsabschnitt (625, 626) umfassen, um einen Datensequenzschlüssel auf der Grundlage einer Datensequenz zu erzeugen, die in die Verschlüsselungsvorrichtung und in die Entschlüsselungsvorrichtung eingegeben oder hiervon ausgegeben wird, und

bei dem der erste und der zweite Abschnitt (609, 610) zum Erzeugen des zeitlich veränderlichen Schlüssels den zeitlich veränderlichen Schlüssel auf der Grundlage der ersten und der zweiten Zufallszahl und des entsprechenden Datensequenzschlüssels erzeugen.

10. Urheberrecht-Schutzsystem nach Anspruch 3, bei dem die Verschlüsselungsvorrichtung ferner einen ersten Abschnitt (103) zum Speichern eines gemeinsamen Schlüssels, um einen gemeinsamen Schlüssel zu speichern, umfasst, die Entschlüsselungsvorrichtung ferner einen zweiten Abschnitt (104) zum Speichern des gemeinsamen Schlüssels, um den gemeinsamen Schlüssel zu speichern, umfasst und die Verschlüsselungsvorrichtung und die Entschlüsselungsvorrichtung ferner el-

nen ersten bzw. einen zweiten Datensequenzschlüssel-Erzeugungsabschnitt (625, 626) umfassen, um einen Datensequenzschlüssel auf der Grundlage einer Datensequenz zu erzeugen, die in die Verschlüsselungsvorrichtung und in die Entschlüsselungsvorrichtung eingegeben oder hiervon ausgegeben wird, und

bei dem der erste und der zweite Abschnitt (609, 610) zum Erzeugen des zeitlich veränderlichen Schlüssels den zeitlich veränderlichen Schlüssel auf der Grundlage der ersten und der zweiten Zufallszahl, des gemeinsamen Schlüssels und des entsprechenden Datensequenzschlüssels erzeugen.

11. Urheberrecht-Schutzsystem nach Anspruch 3, bei dem die Verschlüsselungsvorrichtung und die Entschlüsselungsvorrichtung ferner einen ersten bzw. einen zweiten Datensequenzschlüssel-Erzeugungsabschnitt (625, 626) umfassen, um einen Datensequenzschlüssel auf der Grundlage einer Datensequenz zu erzeugen, der in die Verschlüsselungsvorrichtung und in die Entschlüsselungsvorrichtung eingegeben oder von ihnen ausgegeben wird, und

bei dem der erste und der zweite Inhaltsschlüssel-Erzeugungsabschnitt (617, 618) den Inhaltsschlüssel auf der Grundlage der zweiten Entschlüsselungsbeschränkung und des entsprechenden Datensequenzschlüssels erzeugen.

12. Urheberrecht-Schutzsystem nach Anspruch 3, bei dem die Verschlüsselungsvorrichtung und die Entschlüsselungsvorrichtung ferner einen ersten bzw. einen zweiten Datensequenzschlüssel-Erzeugungsabschnitt (625, 626) umfassen, um einen Datensequenzschlüssel auf der Grundlage einer Datensequenz zu erzeugen, die in die Verschlüsselungsvorrichtung und in die Entschlüsselungsvorrichtung eingegeben bzw. von ihnen ausgegeben wird, und bei dem der erste und der zweite Inhaltsschlüssel-Erzeugungsabschnitt (617, 618) den Inhaltsschlüssel auf der Grundlage der zweiten Entschlüsselungsbeschränkung, des zeitlich veränderlichen Schlüssels und des entsprechenden Datensequenzschlüssels erzeugen.

13. Urheberrecht-Schutzsystem nach Anspruch 3, bei dem der erste und der zweite Abschnitt (107, 108) zur gegenseitigen Authentifizierung die Entschlüsselungsvorrichtung bzw. die Verschlüsselungsvorrichtung durch eine Kommunikation in Übereinstimmung mit einem Authentifizierungsprotokoll des Herausforderungs-Antwort-Typs gegenseitig authentifizieren.

14. Verschlüsselungsvorrichtung zum Ausführen einer verschlüsselten Kommunikation in Verbindung mit

einer Entschlüsselungsvorrichtung unter Verwendung eines Inhaltsschlüssels, die umfasst:

einen Inhaltsspeicherabschnitt (121) zum Speichern von Inhalten;  
einen Inhaltsschlüssel-Erzeugungsabschnitt (117) zum Erzeugen des Inhaltsschlüssels auf der Grundlage einer zweiten Entschlüsselungsbeschränkung, die die Verschlüsselungsvorrichtung von der Entschlüsselungsvorrichtung empfängt und die durch Aktualisieren einer von der Verschlüsselungsvorrichtung empfangenen ersten Entschlüsselungsbeschränkung in Übereinstimmung mit einer Entschlüsselungsbeschränkungs-Aktualisierungsregel erhalten wird; und  
einen ersten Verschlüsselungsabschnitt (119) zum Verschlüsseln der Inhalte unter Verwendung des Inhaltsschlüssels und zum Ausgeben der verschlüsselten Inhalte.

15. Verschlüsselungsvorrichtung nach Anspruch 14, die ferner einen Entschlüsselungsabschnitt (115) umfasst, um die erste verschlüsselte Entschlüsselungsbeschränkung, die von der Entschlüsselungsvorrichtung übertragen wird, unter Verwendung des zeitlich veränderlichen Schlüssels zu entschlüsseln, um die zweite Entschlüsselungsbeschränkung zu erzeugen, und  
der Inhaltsschlüssel-Erzeugungsabschnitt (117) den Inhaltsschlüssel auf der Grundlage der zweiten Entschlüsselungsbeschränkung, die durch die Entschlüsselungsvorrichtung erzeugt wird, erzeugt.

16. Verschlüsselungsvorrichtung nach Anspruch 15, die ferner umfasst:

einen Abschnitt (113) zum Speichern eines gemeinsamen Schlüssels, um einen gemeinsamen Schlüssel zu speichern,  
einen Entschlüsselungsbeschränkungs-Speicherabschnitt (111) zum Speichern der ersten Entschlüsselungsbeschränkung,  
einen ersten Zufallszahl-Erzeugungsabschnitt (105) zum Erzeugen einer ersten Zufallszahl,  
einen Abschnitt (107) zur gegenseitigen Authentifizierung, um eine gegenseitige Authentifizierung in Verbindung mit der Entschlüsselungsvorrichtung unter Verwendung der ersten Zufallszahl und einer von der Entschlüsselungsvorrichtung übertragenen zweiten Zufallszahl auszuführen,  
einen Abschnitt (109) zur Erzeugung eines zeitlich veränderlichen Schlüssels um den zeitlich veränderlichen Schlüssel unter Verwendung der ersten Zufallszahl und der zweiten Zufallszahl in Reaktion auf die Authentifizierung durch

- den Abschnitt zur gegenseitigen Authentifizierung zu erzeugen, und  
einen zweiten Verschlüsselungsabschnitt (113) zum Verschlüsseln der ersten Entschlüsselungsbeschränkung unter Verwendung des zeitlich veränderlichen Schlüssels und zum Ausgeben der zweiten verschlüsselten Entschlüsselungsbeschränkung.
17. Verschlüsselungsvorrichtung nach Anspruch 14, die ferner einen Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt (223) umfasst, um die erste Entschlüsselungsbeschränkung auf die zweite Entschlüsselungsbeschränkung in Übereinstimmung mit einer Entschlüsselungsbeschränkungs-Aktualisierungsregel in Reaktion auf die Aktualisierung einer Entschlüsselungsbeschränkung durch die Entschlüsselungsvorrichtung zu aktualisieren, wobei der Inhaltsschlüssel-Erzeugungsabschnitt (117) den Inhaltsschlüssel auf der Grundlage der zweiten Entschlüsselungsbeschränkung erzeugt, die durch den Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt erhalten wird.
18. Verschlüsselungsvorrichtung nach Anspruch 17, die ferner umfasst:
- einen Abschnitt (103) zum Speichern eines gemeinsamen Schlüssels, um einen gemeinsamen Schlüssel zu speichern,  
einen Entschlüsselungsbeschränkungs-Speicherabschnitt (111) zum Speichern der ersten Entschlüsselungsbeschränkung,  
einen ersten Zufallszahl-Erzeugungsabschnitt (105) zum Erzeugen einer ersten Zufallszahl,  
einen Abschnitt (107) zur gegenseitigen Authentifizierung, um eine gegenseitige Authentifizierung in Verbindung mit der Entschlüsselungsvorrichtung unter Verwendung der ersten Zufallszahl und einer von der Entschlüsselungsvorrichtung übertragenen zweiten Zufallszahl auszuführen,  
einen Abschnitt (109) zum Erzeugen eines zeitlich veränderlichen Schlüssels, um einen zeitlich veränderlichen Schlüssel unter Verwendung der ersten Zufallszahl und der zweiten Zufallszahl in Reaktion auf die Authentifizierung durch den Abschnitt zur gegenseitigen Authentifizierung zu erzeugen, und  
einen zweiten Verschlüsselungsabschnitt (113) zum Verschlüsseln der ersten Entschlüsselungsbeschränkung unter Verwendung des zeitlich veränderlichen Schlüssels und zum Ausgeben einer verschlüsselten Entschlüsselungsbeschränkung.
19. Verschlüsselungsvorrichtung nach Anspruch 14, die ferner einen Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt (323) umfasst, um die erste Entschlüsselungsbeschränkung auf die zweite Entschlüsselungsbeschränkung unabhängig von der Aktualisierung in einer Entschlüsselungsvorrichtung zu aktualisieren;  
wobei der Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt (323) die zweite Entschlüsselungsbeschränkung an den Inhaltsschlüssel-Erzeugungsabschnitt ausgibt;  
der Inhaltsschlüssel-Erzeugungsabschnitt (117) den Inhaltsschlüssel aus der zweiten Entschlüsselungsbeschränkung erzeugt, die durch den Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt erzeugt wird; und  
der Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt (323) die zweite Entschlüsselungsbeschränkung in dem Entschlüsselungsbeschränkungs-Speicherabschnitt in Reaktion auf den Beginn der Verarbeitung durch den ersten Verschlüsselungsabschnitt speichert.
20. Verschlüsselungsvorrichtung nach Anspruch 16, bei der der Abschnitt (109) zur Erzeugung des zeitlich veränderlichen Schlüssels den zeitlich veränderlichen Schlüssel anhand der ersten und der zweiten Zufallszahl und des gemeinsamen Schlüssels erzeugt.
21. Verschlüsselungsvorrichtung nach Anspruch 16, bei der der Inhaltsschlüssel-Erzeugungsabschnitt (117) den Inhaltsschlüssel auf der Grundlage der zweiten Entschlüsselungsbeschränkung und des zeitlich veränderlichen Schlüssels erzeugt.
22. Verschlüsselungsvorrichtung nach Anspruch 16, die ferner einen Datensequenzschlüssel-Erzeugungsabschnitt (625) erzeugt, um einen Datensequenzschlüssel auf der Grundlage einer Datensequenz zu erzeugen, die in die Verschlüsselungsvorrichtung eingegeben oder von ihr ausgegeben wird, wobei der Abschnitt (609) zur Erzeugung des zeitlich veränderlichen Schlüssels den zeitlich veränderlichen Schlüssel auf der Grundlage der ersten und der zweiten Zufallszahl und des Datensequenzschlüssels erzeugt.
23. Verschlüsselungsvorrichtung nach Anspruch 16, die ferner einen Datensequenzschlüssel-Erzeugungsabschnitt (625) umfasst, um einen Datensequenzschlüssel auf der Grundlage einer Datensequenz zu erzeugen, die in die Verschlüsselungsvorrichtung eingegeben oder von ihr ausgegeben wird, wobei der Abschnitt (609) zur Erzeugung des zeitlich veränderlichen Schlüssels den zeitlich veränderlichen Schlüssel auf der Grundlage der ersten und der zweiten Zufallszahl, des gemeinsamen Schlüssels und des Datensequenzschlüssels erzeugt.

24. Verschlüsselungsvorrichtung nach Anspruch 16, die ferner einen Datensequenzschlüssel-Erzeugungsabschnitt (625) umfasst, um einen Datensequenzschlüssel auf der Grundlage einer Datensequenz zu erzeugen, die in die Verschlüsselungsvorrichtung eingegeben oder von ihr ausgegeben wird; wobei der Inhaltesschlüssel-Erzeugungsabschnitt (617) den Inhaltesschlüssel auf der Grundlage der zweiten Entschlüsselungsbeschränkung und des Datensequenzschlüssels erzeugt.

5

10

25. Verschlüsselungsvorrichtung nach Anspruch 16, die ferner einen Datensequenzschlüssel-Erzeugungsabschnitt (625) erzeugt, um einen Datensequenzschlüssel auf der Grundlage einer Datensequenz zu erzeugen, die in die Verschlüsselungsvorrichtung eingegeben oder von ihr ausgegeben wird, wobei der Inhaltesschlüssel-Erzeugungsabschnitt (617) den Inhaltesschlüssel auf der Grundlage der zweiten Entschlüsselungsbeschränkung, des zeitlich veränderlichen Schlüssels und des Datensequenzschlüssels erzeugt.

15

20

26. Entschlüsselungsvorrichtung zum Ausführen einer verschlüsselten Kommunikation in Verbindung mit einer Verschlüsselungsvorrichtung unter Verwendung eines Inhaltesschlüssels, die umfasst:

25

einen Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt (112) zum Empfangen einer ersten Entschlüsselungsbeschränkung und zum Aktualisieren der ersten Entschlüsselungsbeschränkung, um eine zweite Entschlüsselungsbeschränkung in Übereinstimmung mit einer Entschlüsselungsbeschränkungs-Aktualisierungsregel zu erzeugen;

30

einen Inhaltesschlüssel-Erzeugungsabschnitt (118) zum Erzeugen des Inhaltesschlüssels aus der zweiten Entschlüsselungsbeschränkung; und

40

einen ersten Entschlüsselungsabschnitt (120) zum Entschlüsseln verschlüsselter Inhalte unter Verwendung des Inhaltesschlüssels, der durch den Inhaltesschlüssel-Erzeugungsabschnitt erzeugt wird.

45

27. Entschlüsselungsvorrichtung nach Anspruch 26, die ferner umfasst:

einen Verschlüsselungsabschnitt (116) zum Verschlüsseln der zweiten Entschlüsselungsbeschränkung unter Verwendung eines zeitlich veränderlichen Schlüssels und zum Ausgeben der ersten verschlüsselten Entschlüsselungsbeschränkung.

50

55

28. Entschlüsselungsvorrichtung nach Anspruch 27, die ferner umfasst:

einen Abschnitt (104) zum Speichern eines gemeinsamen Schlüssels, um den gemeinsamen Schlüssel zu speichern,

einen Zufallszahl-Erzeugungsabschnitt (106) zum Erzeugen der zweiten Zufallszahl, einen Abschnitt (108) zur gegenseitigen Authentifizierung, um eine gegenseitige Authentifizierung in Verbindung mit der Verschlüsselungsvorrichtung unter Verwendung der zweiten Zufallszahl und einer ersten Zufallszahl auszuführen,

einen Abschnitt (110) zur Erzeugung eines zeitlich veränderlichen Schlüssels, um den zeitlich veränderlichen Schlüssel unter Verwendung der zweiten Zufallszahl und der ersten Zufallszahl in Reaktion auf die Authentifizierung durch den Abschnitt zur gegenseitigen Authentifizierung zu erzeugen, und

einen zweiten Entschlüsselungsabschnitt (114) zum Entschlüsseln einer ersten verschlüsselten Entschlüsselungsbeschränkung unter Verwendung des zeitlich veränderlichen Schlüssels.

29. Entschlüsselungsvorrichtung nach Anspruch 26,

bei der ein Inhaltesschlüssel-Erzeugungsabschnitt (118) zum Erzeugen des Inhaltesschlüssels auf der Grundlage der zweiten Entschlüsselungsbeschränkung, die durch den Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt aktualisiert wird, vorgesehen ist.

30. Entschlüsselungsvorrichtung nach Anspruch 29, die ferner umfasst:

einen zweiten Abschnitt (104) zum Speichern eines gemeinsamen Schlüssels, um den gemeinsamen Schlüssel zu speichern, einen zweiten Zufallszahl-Erzeugungsabschnitt (106) zum Erzeugen der zweiten Zufallszahl,

einen Abschnitt (108) zur gegenseitigen Authentifizierung, um eine gegenseitige Authentifizierung in Verbindung mit der Verschlüsselungsvorrichtung unter Verwendung der zweiten Zufallszahl und der ersten Zufallszahl auszuführen,

einen Abschnitt (110) zur Erzeugung eines zeitlich veränderlichen Schlüssels, um den zeitlich veränderlichen Schlüssel unter Verwendung der zweiten Zufallszahl und der ersten Zufallszahl in Reaktion auf die Authentifizierung durch den Abschnitt zur gegenseitigen Authentifizierung zu erzeugen, und

einen zweiten Entschlüsselungsabschnitt (114) zum Entschlüsseln einer verschlüsselten Entschlüsselungsbeschränkung unter Verwendung des zeitlich veränderlichen Schlüssels.

31. Entschlüsselungsvorrichtung nach Anspruch 28, bei der der Abschnitt (110) zur Erzeugung des zeitlich veränderlichen Schlüssels den zeitlich veränderlichen Schlüssel auf der Grundlage der ersten und der zweiten Zufallszahl und des gemeinsamen Schlüssels erzeugt. 5
32. Entschlüsselungsvorrichtung nach Anspruch 28, bei der der Inhaltesschlüssel-Erzeugungsabschnitt (118) den Inhaltesschlüssel auf der Grundlage der zweiten Entschlüsselungsbeschränkung und des zeitlich veränderlichen Schlüssels erzeugt. 10
33. Entschlüsselungsvorrichtung nach Anspruch 28, die ferner einen Datensequenzschlüssel-Erzeugungsabschnitt (626) umfasst, um einen Datensequenzschlüssel auf der Grundlage einer Datensequenz zu erzeugen, die in die Entschlüsselungsvorrichtung eingegeben oder von ihr ausgegeben wird, wobei der Abschnitt (610) zur Erzeugung des zeitlich veränderlichen Schlüssels den zeitlich veränderlichen Schlüssel auf der Grundlage der ersten und der zweiten Zufallszahl und des Datensequenzschlüssels erzeugt. 15  
20  
25
34. Entschlüsselungsvorrichtung nach Anspruch 28, die ferner einen Datensequenzschlüssel-Erzeugungsabschnitt (626) umfasst, um einen Datensequenzschlüssel auf der Grundlage einer Datensequenz zu erzeugen, die in die Entschlüsselungsvorrichtung eingegeben oder von ihr ausgegeben wird, wobei der Abschnitt (610) zur Erzeugung des zeitlich veränderlichen Schlüssels den zeitlich veränderlichen Schlüssel auf der Grundlage der ersten und der zweiten Zufallszahl, des gemeinsamen Schlüssels und des Datensequenzschlüssels erzeugt. 30  
35
35. Entschlüsselungsvorrichtung nach Anspruch 28, die ferner einen Datensequenzschlüssel-Erzeugungsabschnitt (626) umfasst, um einen Datensequenzschlüssel auf der Grundlage einer Datensequenz zu erzeugen, die in die Entschlüsselungsvorrichtung eingegeben oder von ihr ausgegeben wird, wobei der Inhaltesschlüssel-Erzeugungsabschnitt (618) den Inhaltesschlüssel auf der Grundlage der zweiten Entschlüsselungsbeschränkung und des Datensequenzschlüssels erzeugt. 40
36. Entschlüsselungsvorrichtung nach Anspruch 28, die ferner einen Datensequenzschlüssel-Erzeugungsabschnitt (626) umfasst, um einen Datensequenzschlüssel auf der Grundlage einer Datensequenz zu erzeugen, die in die Entschlüsselungsvorrichtung eingegeben oder von ihr ausgegeben wird, wobei der Inhaltesschlüssel-Erzeugungsabschnitt (618) den Inhaltesschlüssel auf der Grundlage der zweiten Entschlüsselungsbeschränkung, 50  
55
- des zeitlich veränderlichen Schlüssels und des Datensequenzschlüssels erzeugt.
37. Aufzeichnungsmedium, das ein Programm speichert, das dazu verwendet wird, einen Computer dazu zu veranlassen, eine verschlüsselte Kommunikation mit einer Verschlüsselungsvorrichtung unter Verwendung eines Inhaltesschlüssels auszuführen, wobei:
- das Programm den Computer dazu veranlasst, dass er arbeitet als:
- ein Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt (112) zum Empfangen einer ersten Entschlüsselungsbeschränkung und zum Aktualisieren der ersten Entschlüsselungsbeschränkung, um eine zweite Entschlüsselungsbeschränkung in Übereinstimmung mit einer Entschlüsselungsbeschränkungs-Aktualisierungsregel zu erzeugen;
- ein Inhaltesschlüssel-Erzeugungsabschnitt (118) zum Erzeugen des Inhaltesschlüssels aus der zweiten Entschlüsselungsbeschränkung; und
- ein erster Entschlüsselungsabschnitt (120) zum Entschlüsseln verschlüsselter Inhalte unter Verwendung des Inhaltesschlüssels, der durch den Inhaltesschlüssel-Erzeugungsabschnitt erzeugt wird.
38. Aufzeichnungsmedium nach Anspruch 37, bei dem das Programm den Computer dazu veranlasst, ferner zu arbeiten als:
- ein Verschlüsselungsabschnitt (116) zum Verschlüsseln der zweiten Entschlüsselungsbeschränkung unter Verwendung eines zeitlich veränderlichen Schlüssels und zum Ausgeben einer ersten entschlüsselten Entschlüsselungsbeschränkung.
39. Aufzeichnungsmedium nach Anspruch 38, bei dem das Programm den Computer dazu veranlasst, ferner zu arbeiten als:
- ein Abschnitt (104) zum Speichern eines gemeinsamen Schlüssels, um den gemeinsamen Schlüssel zu speichern;
- ein Zufallszahl-Erzeugungsabschnitt (106) zum Erzeugen einer zweiten Zufallszahl;
- ein Abschnitt (108) zur gegenseitigen Authentifizierung, um eine gegenseitige Authentifizierung in Verbindung mit der Verschlüsselungsvorrichtung unter Verwendung der zweiten Zufallszahl und einer ersten Zufallszahl auszuführen;

- ein Abschnitt (110) zur Erzeugung eines zeitlich veränderlichen Schlüssels, um den zeitlich veränderlichen Schlüssel unter Verwendung der zweiten Zufallszahl und der ersten Zufallszahl in Reaktion auf die Authentifizierung durch den Abschnitt zur gegenseitigen Authentifizierung zu erzeugen; und  
 ein zweiter Entschlüsselungsabschnitt (114) zum Entschlüsseln einer ersten verschlüsselten Entschlüsselungsbeschränkung unter Verwendung des zeitlich veränderlichen Schlüssels.
40. Aufzeichnungsmedium nach Anspruch 37, bei dem:  
 das Programm den Computer dazu veranlasst, ferner zu arbeiten als ein Inhaltsschlüssel-Erzeugungsabschnitt (118) zum Erzeugen des Inhaltsschlüssels anhand der zweiten Entschlüsselungsbeschränkung, die durch den Entschlüsselungsbeschränkungs-Aktualisierungsabschnitt erhalten wird.
41. Aufzeichnungsmedium nach Anspruch 40, bei dem das Programm den Computer dazu veranlasst, ferner zu arbeiten als:  
 einen zweiten Abschnitt (104) zum Speichern des gemeinsamen Schlüssels, um den gemeinsamen Schlüssel zu speichern;  
 einen zweiten Zufallszahl-Erzeugungsabschnitt (106) zum Erzeugen der zweiten Zufallszahl;  
 einen Abschnitt (108) zur gegenseitigen Authentifizierung, um eine gegenseitige Authentifizierung in Verbindung mit der Verschlüsselungsvorrichtung unter Verwendung der zweiten Zufallszahl und der ersten Zufallszahl auszuführen;  
 einen Abschnitt (110) zur Erzeugung eines zeitlich veränderlichen Schlüssels, um einen zeitlich veränderlichen Schlüssel unter Verwendung der zweiten Zufallszahl und der ersten Zufallszahl in Reaktion auf die Authentifizierung durch den Abschnitt zur gegenseitigen Authentifizierung zu erzeugen; und  
 einen zweiten Entschlüsselungsabschnitt (114) zum Entschlüsseln einer verschlüsselten Entschlüsselungsbeschränkung unter Verwendung des zeitlich veränderlichen Schlüssels.
42. Aufzeichnungsmedium nach Anspruch 39, bei dem der Abschnitt (110) zur Erzeugung eines zeitlich veränderlichen Schlüssels den zeitlich veränderlichen Schlüssel anhand der ersten und der zweiten Zufallszahl und des gemeinsamen Schlüssels erzeugt.
43. Aufzeichnungsmedium nach Anspruch 39, bei dem der Inhaltsschlüssel-Erzeugungsabschnitt (118) den Inhaltsschlüssel auf der Grundlage der zweiten Entschlüsselungsbeschränkung und des zeitlich veränderlichen Schlüssels erzeugt.
44. Aufzeichnungsmedium nach Anspruch 39, bei dem:  
 das Programm den Computer dazu veranlasst, ferner zu arbeiten als ein Datensequenzschlüssel-Erzeugungsabschnitt (626) zum Erzeugen eines Datensequenzschlüssels auf der Grundlage einer Datensequenz, die in die Entschlüsselungsvorrichtung eingegeben oder von ihr ausgegeben wird; und  
 der Abschnitt (610) zur Erzeugung des zeitlich veränderlichen Schlüssels den zeitlich veränderlichen Schlüssel auf der Grundlage der ersten und der zweiten Zufallszahl und des Datensequenzschlüssels erzeugt.
45. Aufzeichnungsmedium nach Anspruch 39, bei dem:  
 das Programm den Computer dazu veranlasst, ferner zu arbeiten als ein Datensequenzschlüssel-Erzeugungsabschnitt (626) zum Erzeugen eines Datensequenzschlüssels auf der Grundlage einer Datensequenz, die in eine Entschlüsselungsvorrichtung eingegeben oder von ihr ausgegeben wird; und  
 der Abschnitt (610) zur Erzeugung des zeitlich veränderlichen Schlüssels den zeitlich veränderlichen Schlüssel auf der Grundlage der ersten und der zweiten Zufallszahl, des gemeinsamen Schlüssels und des Datensequenzschlüssels erzeugt.
46. Aufzeichnungsmedium nach Anspruch 39, bei dem:  
 das Programm den Computer dazu veranlasst, ferner zu arbeiten als ein Datensequenzschlüssel-Erzeugungsabschnitt (626) zum Erzeugen eines Datensequenzschlüssels auf der Grundlage einer Datensequenz, die in eine Entschlüsselungsvorrichtung eingegeben oder von ihr ausgegeben wird; und  
 der Inhaltsschlüssel-Erzeugungsabschnitt (618) den Inhaltsschlüssel auf der Grundlage der zweiten Entschlüsselungsbeschränkung und des Datensequenzschlüssels erzeugt.
47. Aufzeichnungsmedium nach Anspruch 39, bei dem:  
 das Programm den Computer dazu veranlasst, ferner zu arbeiten als ein Datensequenzschlüssel-Erzeugungsabschnitt (626) zum Erzeugen eines Datensequenzschlüssels auf der Grundlage einer Datensequenz, die in eine Ent-



schlüsselungsvorrichtung eingegeben oder von ihr ausgegeben wird; und der Inhabeschlüssel-Erzeugungsabschnitt (618) den Inhabeschlüssel auf der Grundlage der zweiten Entschlüsselungsbeschränkung, des zeitlich veränderlichen Schlüssels und des Datensequenzschlüssels erzeugt.

## Revendications

### 1. Système de protection de copyright comprenant :

un dispositif de cryptage (101) et un dispositif de décryptage (102), dans lesquels une communication cryptographique est exécutée entre le dispositif de cryptage et le dispositif de décryptage en utilisant une clé de contenu,

dans lequel le dispositif de cryptage comprend

une section de mémorisation de contenu (121) destinée à mémoriser un contenu,

une première section de génération de clé de contenu (117) destinée à générer la clé de contenu sur la base d'une seconde limitation de décryptage obtenue en mettant à jour une première limitation de décryptage conformément à une règle de mise à jour de limitation de décryptage, et

une première section de cryptage (119) destinée à crypter le contenu en utilisant la clé de contenu et à fournir en sortie le contenu crypté, et

dans lequel le dispositif de décryptage comprend

une seconde section de génération de clé de contenu (118) destinée à générer la clé de contenu à partir de la seconde limitation de décryptage, et

une première section de décryptage (120) destinée à décrypter le contenu crypté en utilisant la clé de contenu générée par la seconde section de génération de clé de contenu.

### 2. Système de protection de copyright selon la revendication 1, dans lequel le dispositif de décryptage comprend en outre

une section de mise à jour de limitation de décryptage (112) destinée à mettre à jour la première limitation de décryptage pour la seconde limitation de décryptage conformément à une règle de mise à jour de limitation de décryptage, et

une seconde section de cryptage (116) destinée à crypter la seconde limitation de décryptage en utilisant une clé variable dans le temps, et à fournir en sortie la première limitation de décryptage cryptée,

dans lequel le dispositif de cryptage comprend en outre une seconde section de décryptage (115) destinée à décrypter la première limitation de

décryptage cryptée transférée depuis la seconde section de cryptage en utilisant la clé variable dans le temps pour générer la seconde limitation de décryptage,

dans lequel la première section de génération de clé de contenu (117) génère la clé de contenu sur la base de la seconde limitation de décryptage générée par la seconde section de décryptage.

### 3. Système de protection de copyright selon la revendication 2, dans lequel le dispositif de cryptage comprend en outre

une section de mémorisation de limitation de décryptage (111) destinée à mémoriser la première limitation de décryptage,

une première section de génération de nombre aléatoire (105) destinée à générer un premier nombre aléatoire,

une première section d'authentification mutuelle (107) destinée à exécuter une authentification mutuelle en association avec le dispositif de décryptage utilisant le premier nombre aléatoire, et un second nombre aléatoire transféré depuis le dispositif de décryptage,

une première section de génération de clé variable dans le temps (109) destinée à générer la clé variable dans le temps en utilisant le premier nombre aléatoire et le second nombre aléatoire en réponse à l'authentification par la première section d'authentification mutuelle, et

une troisième section de cryptage (113) destinée à crypter la première limitation de décryptage en utilisant la clé variable dans le temps et à fournir en sortie la seconde limitation de décryptage cryptée, et

dans lequel le dispositif de décryptage comprend en outre

une seconde section de génération de nombre aléatoire (106) destinée à générer le second nombre aléatoire,

une seconde section d'authentification mutuelle (108) destinée à exécuter une authentification mutuelle en association avec le dispositif de cryptage en utilisant le second nombre aléatoire et le premier nombre aléatoire,

une seconde section de génération de clé variable dans le temps (110) destinée à générer la clé variable dans le temps en utilisant le second nombre aléatoire et le premier nombre aléatoire en réponse à l'authentification par la seconde section d'authentification mutuelle, et

une troisième section de décryptage (114) destinée à décrypter la seconde limitation de décryptage cryptée en utilisant la clé variable dans le temps.

### 4. Système de protection de copyright selon la revendication 1, dans lequel le dispositif de décryptage

comprend en outre une première section de mise à jour de limitation de décryptage (212) destinée à mettre à jour la première limitation de décryptage pour la seconde limitation de décryptage conformément à une règle de mise à jour de limitation de décryptage, et

une seconde section de génération de clé de contenu (118) destinée à générer la clé de contenu sur la base de la seconde limitation de décryptage mise à jour par la première section de mise à jour de limitation de décryptage,

dans lequel le dispositif de cryptage comprend en outre une seconde section de mise à jour de limitation de décryptage (223) destinée à mettre à jour la première limitation de décryptage pour la seconde limitation de décryptage conformément à la règle de mise à jour de limitation de décryptage en réponse à la mise à jour de la première limitation de décryptage par la première section de mise à jour de limitation de décryptage,

la première section de génération de clé de contenu (117) génère la clé de contenu sur la base de la seconde limitation de décryptage mise à jour par la seconde section de mise à jour de limitation de décryptage.

5. Système de protection de copyright selon la revendication 4, dans lequel le dispositif de cryptage comprend en outre

une section de mémorisation de limitation de décryptage (211) destinée à mémoriser la première limitation de décryptage,

une première section de génération de nombre aléatoire (105) destinée à générer un premier nombre aléatoire,

une première section d'authentification mutuelle (107) destinée à exécuter une authentification mutuelle en association avec le dispositif de décryptage en utilisant le premier nombre aléatoire, et un second nombre aléatoire transféré depuis le dispositif de décryptage,

une première section de génération de clé variable dans le temps (109) destinée à générer une clé variable dans le temps en utilisant le premier nombre aléatoire et le second nombre aléatoire en réponse à l'authentification par la première section d'authentification mutuelle, et

une seconde section de cryptage (113) destinée à crypter la première limitation de décryptage en utilisant la clé variable dans le temps et à fournir en sortie une limitation de décryptage cryptée, et

dans lequel le dispositif de décryptage comprend en outre

une seconde section de génération de nombre aléatoire (106) destinée à générer le second nombre aléatoire,

une seconde section d'authentification mutuelle (108) destinée à exécuter une authentifica-

tion mutuelle en association avec le dispositif de cryptage en utilisant le second nombre aléatoire et le premier nombre aléatoire,

une seconde section de génération de clé variable dans le temps (110) destinée à générer la clé variable dans le temps en utilisant le second nombre aléatoire et le premier nombre aléatoire en réponse à l'authentification par la seconde section d'authentification mutuelle, et

une seconde section de décryptage (114) destinée à décrypter la limitation de décryptage cryptée en utilisant la clé variable dans le temps.

6. Système de protection de copyright selon la revendication 1, dans lequel le dispositif de cryptage comprend en outre une seconde section de mise à jour de limitation de décryptage (323) destinée à mettre à jour la première limitation de décryptage pour la seconde limitation de décryptage indépendamment d'une mise à jour par la première section de limitation de décryptage,

la première section de génération de clé de contenu (117) génère la clé de contenu à partir de la seconde limitation de décryptage mise à jour par la seconde section de mise à jour de limitation de décryptage (323), et

la seconde section de mise à jour de limitation de décryptage (323) mémorise la seconde limitation de décryptage dans la section de mémorisation de limitation de décryptage en réponse au début du traitement par la première section de cryptage.

7. Système de protection de copyright selon la revendication 3, dans lequel le dispositif de cryptage comprend en outre une première section de mémorisation de clé commune (103) destinée à mémoriser une clé commune, le dispositif de décryptage comprend en outre une seconde section de mémorisation de clé commune (104) destinée à mémoriser la clé commune, et les première et seconde sections de génération de clé variable dans le temps (109, 110) génèrent la clé variable dans le temps sur la base des premier et second nombres aléatoires et de la clé commune.

8. Système de protection de copyright selon la revendication 3, dans lequel les première et seconde sections de génération de clé de contenu (117, 118) génèrent la clé de contenu sur la base de la seconde limitation de décryptage et de la clé variable dans le temps.

9. Système de protection de copyright selon la revendication 3, dans lequel le dispositif de cryptage et le dispositif de décryptage comprennent en outre des première et seconde sections de génération de clé de séquence de données respectives (625, 626) destinées à générer une clé de séquence de don-

nées sur la base d'une séquence de données appliquée en entrée au dispositif de cryptage et au dispositif de décryptage ou fournie en sortie depuis ceux-ci, et

dans lequel les première et seconde sections de génération de clé variable dans le temps (609, 610) génèrent la clé variable dans le temps sur la base des premier et second nombres aléatoires et de la clé de séquence de données respective.

10. Système de protection de copyright selon la revendication 3, dans lequel le dispositif de cryptage comprend en outre une première section de mémorisation de clé commune (103) destinée à mémoriser une clé commune, le dispositif de décryptage comprend en outre une seconde section de mémorisation de clé commune (104) destinée à mémoriser la clé commune, et le dispositif de cryptage ainsi que le dispositif de décryptage comprennent en outre des première et seconde sections de génération de clé de séquence de données (625, 626) destinées à générer une clé de séquence de données sur la base d'une séquence de données appliquée en entrée au dispositif de cryptage et au dispositif de décryptage ou fournie en sortie à partir de ceux-ci, et

dans lequel les première et seconde sections de génération de clé variable dans le temps (609, 610) génèrent la clé variable dans le temps sur la base des premier et second nombres aléatoires, de la clé commune, et de la clé de séquence de données respective.

11. Système de protection de copyright selon la revendication 3, dans lequel le dispositif de cryptage et le dispositif de décryptage comprennent en outre des première et seconde sections de génération de clé de séquence de données respectives (625, 626) destinées à générer une clé de séquence de données sur la base d'une séquence de données appliquée en entrée au dispositif de cryptage et au dispositif de décryptage ou fournie en sortie à partir de ceux-ci, et

dans lequel les première et seconde sections de génération de clé de contenu (617, 618) génèrent la clé de contenu sur la base de la seconde limitation de décryptage et de la clé de séquence de données respective.

12. Système de protection de copyright selon la revendication 3, dans lequel le dispositif de cryptage et le dispositif de décryptage comprennent en outre des première et seconde sections de génération de clé de séquence de données respectives (625, 626) destinées à générer une clé de séquence de données sur la base d'une séquence de données appliquée en entrée au dispositif de cryptage et au dispositif de décryptage ou fournie en sortie de ceux-

ci, et dans lequel les première et seconde sections de génération de clé de contenu (617, 618) génèrent la clé de contenu sur la base de la seconde limitation de décryptage, de la clé variable dans le temps, et de la clé de séquence de données respective.

13. Système de protection de copyright selon la revendication 3, dans lequel les première et seconde sections d'authentification mutuelle (107, 108) authentifient mutuellement le dispositif de décryptage et le dispositif de cryptage, respectivement, par une communication conformément à un protocole d'authentification du type demande-réponse.
14. Dispositif de cryptage destiné à exécuter une communication cryptographique en association avec un dispositif de décryptage en utilisant une clé de contenu, comprenant :

une section de mémorisation de contenu (121) destinée à mémoriser un contenu,  
une section de génération de clé de contenu (117) destinée à générer la clé de contenu sur la base d'une seconde limitation de décryptage reçue par le dispositif de cryptage depuis le dispositif de décryptage, obtenue en mettant à jour une première limitation de décryptage reçue du dispositif de cryptage conformément à une règle de mise à jour de limitation de décryptage, et  
une première section de cryptage (119) destinée à crypter le contenu en utilisant la clé de contenu et à fournir en sortie le contenu crypté.

15. Dispositif de cryptage selon la revendication 14, comprenant en outre une section de décryptage (115) destinée à décrypter la première limitation de décryptage cryptée transférée depuis le dispositif de décryptage en utilisant la clé variable dans le temps pour générer la seconde limitation de décryptage, et

la section de génération de clé de contenu (117) génère la clé de contenu sur la base de la seconde limitation de décryptage générée par le dispositif de décryptage.

16. Dispositif de cryptage selon la revendication 15, comprenant en outre

une section de mémorisation de clé commune (103) destinée à mémoriser une clé commune,  
une section de mémorisation de limitation de décryptage (111) destinée à mémoriser la première limitation de décryptage,  
une première section de génération de nombre aléatoire (105) destinée à générer un premier nombre aléatoire,  
une section d'authentification mutuelle (107)

- destinée à exécuter une authentification mutuelle en association avec le dispositif de décryptage en utilisant le premier nombre aléatoire, et un second nombre aléatoire transféré depuis le dispositif de décryptage,
- une section de génération de clé variable dans le temps (109) destinée à générer la clé variable dans le temps en utilisant le premier nombre aléatoire et le second nombre aléatoire en réponse à l'authentification par la section d'authentification mutuelle, et
- une seconde section de cryptage (113) destinée à crypter la première limitation de décryptage en utilisant la clé variable dans le temps et à fournir en sortie la seconde limitation de décryptage cryptée.
17. Dispositif de cryptage selon la revendication 14, comprenant en outre une section de mise à jour de limitation de décryptage (223) destinée à mettre à jour la première limitation de décryptage pour la seconde limitation de décryptage conformément à une règle de mise à jour de limitation de décryptage en réponse à la mise à jour d'une limitation de décryptage par le dispositif de décryptage,
- dans lequel la section de génération de clé de contenu (117) génère la clé de contenu sur la base de la seconde limitation de décryptage obtenue par la section de mise à jour de limitation de décryptage.
18. Dispositif de cryptage selon la revendication 17, comprenant en outre
- une section de mémorisation de clé commune (103) destinée à mémoriser une clé commune,
- une section de mémorisation de limitation de décryptage (111) destinée à mémoriser la première limitation de décryptage,
- une première section de génération de nombre aléatoire (105) destinée à générer un premier nombre aléatoire,
- une section d'authentification mutuelle (107) destinée à exécuter une authentification mutuelle en association avec le dispositif de décryptage en utilisant le premier nombre aléatoire, et un second nombre aléatoire transféré depuis le dispositif de décryptage,
- une section de génération de clé variable dans le temps (109) destinée à générer une clé variable dans le temps en utilisant le premier nombre aléatoire et le second nombre aléatoire en réponse à l'authentification par la section d'authentification mutuelle, et
- une seconde section de cryptage (113) destinée à crypter la première limitation de décryptage en utilisant la clé variable dans le temps et à fournir en sortie une limitation de décryptage cryptée.
19. Dispositif de cryptage selon la revendication 14, comprenant en outre une section de mise à jour de limitation de décryptage (323) destinée à mettre à jour la première limitation de décryptage pour la seconde limitation de décryptage indépendamment de la mise à jour dans un dispositif de décryptage,
- la section de mise à jour de limitation de décryptage (323) fournit en sortie la seconde limitation de décryptage à la section de génération de clé de contenu,
- la section de génération de clé de contenu (117) génère la clé de contenu à partir de la seconde limitation de décryptage générée par la section de mise à jour de limitation de décryptage, et
- la section de mise à jour de limitation de décryptage (323) mémorise la seconde limitation de décryptage dans la section de mémorisation de limitation de décryptage en réponse au début du traitement par la première section de cryptage.
20. Dispositif de cryptage selon la revendication 16, dans lequel la section de génération de clé variable dans le temps (109) génère la clé variable dans le temps sur la base des premier et second nombres aléatoires et de la clé commune.
21. Dispositif de cryptage selon la revendication 16, dans lequel la section de génération de clé de contenu (117) génère la clé de contenu sur la base de la seconde limitation de décryptage et de la clé variable dans le temps.
22. Dispositif de cryptage selon la revendication 16, comprenant en outre une section de génération de clé de séquence de données (625) destinée à générer une clé de séquence de données sur la base d'une séquence de données appliquée en entrée au dispositif de cryptage ou fournie en sortie depuis celui-ci,
- la section de génération de clé variable dans le temps (609) génère la clé variable dans le temps sur la base des premier et second nombres aléatoires et de la clé de séquence de données.
23. Dispositif de cryptage selon la revendication 16, comprenant en outre une section de génération de clé de séquence de données (625) destinée à générer une clé de séquence de données sur la base d'une séquence de données appliquée en entrée au dispositif de cryptage ou fournie en sortie depuis celui-ci,
- dans lequel la section de génération de clé variable dans le temps (609) génère la clé variable dans le temps sur la base des premier et second nombres aléatoires, de la clé commune, et de la clé de séquence de données.
24. Dispositif de cryptage selon la revendication 16,

- comprenant en outre une section de génération de clé de séquence de données (625) destinée à générer une clé de séquence de données sur la base d'une séquence de données appliquée en entrée au dispositif de cryptage ou fournie en sortie depuis celui-ci,
- dans lequel la section de génération de clé de contenu (617) génère la clé de contenu sur la base de la seconde limitation de décryptage et de la clé de séquence de données.
25. Dispositif de cryptage selon la revendication 16, comprenant en outre une section de génération de clé de séquence de données (625) destinée à générer une clé de séquence de données sur la base d'une séquence de données appliquée en entrée au dispositif de cryptage ou fournie en sortie depuis celui-ci,
- dans lequel la section de génération de clé de contenu (617) génère la clé de contenu sur la base de la seconde limitation de décryptage, de la clé variable dans le temps, et de la clé de séquence de données.
26. Dispositif de décryptage destiné à exécuter une communication cryptographique en association avec un dispositif de cryptage en utilisant une clé de contenu, comprend :
- une section de mise à jour de limitation de décryptage (112) destinée à recevoir une première limitation de décryptage et destinée à mettre à jour la première limitation de décryptage pour générer une seconde limitation de décryptage conformément à une règle de mise à jour de limitation de décryptage,
- une section de génération de clé de contenu (118) destinée à générer la clé de contenu à partir de la seconde limitation de décryptage, et une première section de décryptage (120) destinée à décrypter un contenu crypté en utilisant la clé de contenu générée par la section de génération de clé de contenu.
27. Dispositif de décryptage selon la revendication 26, comprenant en outre
- une section de cryptage (116) destinée à crypter la seconde limitation de décryptage en utilisant une clé variable dans le temps, et à fournir en sortie la première limitation de décryptage cryptée.
28. Dispositif de décryptage selon la revendication 27, comprenant en outre
- une section de mémorisation de clé commune (104) destinée à mémoriser la clé commune,
- une section de génération de nombre aléatoire (106) destinée à générer le second nombre aléatoire,
- une section d'authentification mutuelle (108) destinée à exécuter une authentification mutuelle en association avec le dispositif de cryptage en utilisant le second nombre aléatoire et un premier nombre aléatoire,
- une section de génération de clé variable dans le temps (110) destinée à générer la clé variable dans le temps en utilisant le second nombre aléatoire et le premier nombre aléatoire en réponse à l'authentification par la section d'authentification mutuelle, et
- une seconde section de décryptage (114) destinée à décrypter une première limitation de décryptage cryptée en utilisant la clé variable dans le temps.
29. Dispositif de décryptage selon la revendication 26, dans lequel une section de génération de clé de contenu (118) est destinée à générer la clé de contenu sur la base de la seconde limitation de décryptage mise à jour par la section de mise à jour de limitation de décryptage.
30. Dispositif de décryptage selon la revendication 29, comprenant en outre
- une seconde section de mémorisation de clé commune (104) destinée à mémoriser la clé commune,
- une seconde section de génération de nombre aléatoire (106) destinée à générer le second nombre aléatoire,
- une section d'authentification mutuelle (108) destinée à exécuter une authentification mutuelle en association avec le dispositif de cryptage en utilisant le second nombre aléatoire et un premier nombre aléatoire,
- une section de génération de clé variable dans le temps (110) destinée à générer la clé variable dans le temps en utilisant le second nombre aléatoire et le premier nombre aléatoire en réponse à l'authentification par la section d'authentification mutuelle, et
- une seconde section de décryptage (114) destinée à décrypter une limitation de décryptage cryptée en utilisant la clé variable dans le temps.
31. Dispositif de décryptage selon la revendication 28, dans lequel la section de génération de clé variable dans le temps (110) génère la clé variable dans le temps sur la base des premier et second nombres aléatoires et de la clé commune.
32. Dispositif de décryptage selon la revendication 28, dans lequel la section de génération de clé de contenu (118) génère la clé de contenu sur la base de la seconde limitation de décryptage et de la clé variable dans le temps.

33. Dispositif de décryptage selon la revendication 28, comprenant en outre une section de génération de clé de séquence de données (626) destinée à générer une clé de séquence de données sur la base d'une séquence de données appliquée en entrée au dispositif de décryptage ou fournie en sortie depuis celui-ci, dans lequel la section de génération de clé variable dans le temps (610) génère la clé variable dans le temps sur la base des premier et second nombres aléatoires et de la clé de séquence de données.
34. Dispositif de décryptage selon la revendication 28, comprenant en outre une section de génération de clé de séquence de données (626) destinée à générer une clé de séquence de données sur la base d'une séquence de données appliquée en entrée au dispositif de décryptage ou fournie en sortie depuis celui-ci, dans lequel la section de génération de clé variable dans le temps (610) génère la clé variable dans le temps sur la base des premier et second nombres aléatoires, de la clé commune, et de la clé de séquence de données.
35. Dispositif de décryptage selon la revendication 28, comprenant en outre une section de génération de clé de séquence de données (626) destinée à générer une clé de séquence de données sur la base d'une séquence de données appliquée en entrée au dispositif de décryptage ou fournie en sortie depuis celui-ci, dans lequel la section de génération de clé de contenu (618) génère la clé de contenu sur la base de la seconde limitation de décryptage et de la clé de séquence de données.
36. Dispositif de décryptage selon la revendication 28, comprenant en outre une section de génération de clé de séquence de données (626) destinée à générer une clé de séquence de données sur la base d'une séquence de données appliquée en entrée au dispositif de décryptage ou fournie en sortie depuis celui-ci, dans lequel la section de génération de clé de contenu (618) génère la clé de contenu sur la base de la seconde limitation de décryptage, de la clé variable dans le temps, et de la clé de séquence de données.
37. Support de mémorisation mémorisant un programme destiné à être utilisé pour amener un ordinateur à exécuter une communication cryptographique avec un dispositif de cryptage en utilisant une clé de contenu, dans lequel :
- le programme amène l'ordinateur à fonctionner
- comme :
- une section de mise à jour de limitation de décryptage (112) destinée à recevoir une première limitation de décryptage et destinée à mettre à jour la première limitation de décryptage pour générer une seconde limitation de décryptage conformément à une règle de mise à jour de limitation de décryptage, une section de génération de clé de contenu (118) destinée à générer la clé de contenu à partir de la seconde limitation de décryptage, et une première section de décryptage (120) destinée à décrypter un contenu crypté en utilisant la clé de contenu générée par la section de génération de clé de contenu.
38. Support d'enregistrement selon la revendication 37, dans lequel le programme amène l'ordinateur à fonctionner en outre comme :
- une section de cryptage (116) destinée à crypter la seconde limitation de décryptage en utilisant une clé variable dans le temps, et à fournir en sortie une première limitation de décryptage cryptée.
39. Support d'enregistrement selon la revendication 38, dans lequel le programme amène l'ordinateur à fonctionner en outre comme :
- une section de mémorisation de clé commune (104) destinée à mémoriser la clé commune, une section de génération de nombre aléatoire (106) destinée à générer un second nombre aléatoire, une section d'authentification mutuelle (108) destinée à exécuter une authentification mutuelle en association avec le dispositif de cryptage en utilisant le second nombre aléatoire et un premier nombre aléatoire, une section de génération de clé variable dans le temps (110) destinée à la génération de la clé variable dans le temps en utilisant le second nombre aléatoire et le premier nombre aléatoire en réponse à l'authentification par la section d'authentification mutuelle, et une seconde section de décryptage (114) destinée à décrypter une première limitation de décryptage cryptée en utilisant la clé variable dans le temps.
40. Support d'enregistrement selon la revendication 37, dans lequel :
- le programme amène l'ordinateur à fonctionner

en outre comme une section de génération de clé de contenu (118) destinée à générer la clé de contenu sur la base de la seconde limitation de décryptage obtenue par la section de mise à jour de limitation de décryptage.

41. Support d'enregistrement selon la revendication 40, dans lequel le programme amène l'ordinateur à fonctionner en outre comme :

une seconde section de mémorisation de clé commune (104) destinée à mémoriser la clé commune,

une seconde section de génération de nombre aléatoire (106) destinée à générer le second nombre aléatoire,

une section d'authentification mutuelle (108) destinée à exécuter une authentification mutuelle en association avec le dispositif de cryptage en utilisant le second nombre aléatoire et un premier nombre aléatoire,

une section de génération de clé variable dans le temps (110) destinée à générer une clé variable dans le temps en utilisant le second nombre aléatoire et le premier nombre aléatoire en réponse à l'authentification par la section d'authentification mutuelle, et

une seconde section de décryptage (114) destinée à décrypter une limitation de décryptage cryptée en utilisant la clé variable dans le temps.

42. Support d'enregistrement selon la revendication 39, dans lequel la section de génération de clé variable dans le temps (110) génère la clé variable dans le temps sur la base des premier et second nombres aléatoires et de la clé commune.

43. Support d'enregistrement selon la revendication 39, dans lequel la section de génération de clé de contenu (118) génère la clé de contenu sur la base de la seconde limitation de décryptage et de la clé variable dans le temps.

44. Support d'enregistrement selon la revendication 39, dans lequel :

le programme amène l'ordinateur à fonctionner en outre comme une section de génération de clé de séquence de données (626) destinée à générer une clé de séquence de données sur la base d'une séquence de données appliquée en entrée à un dispositif de décryptage ou fournie en sortie depuis celui-ci, et

la section de génération de clé variable dans le temps (610) génère la clé variable dans le temps sur la base des premier et second nombres aléatoires et de la clé de séquence de données.

nées.

45. Support d'enregistrement selon la revendication 39, dans lequel :

le programme amène l'ordinateur à fonctionner en outre comme une section de génération de clé de séquence (626) destinée à générer une clé de séquence sur la base d'une séquence de données appliquée en entrée à un dispositif de décryptage ou fournie en sortie depuis celui-ci, et

la section de génération de clé variable dans le temps (610) génère la clé variable dans le temps sur la base des premier et second nombres aléatoires, de la clé commune, et de la clé de séquence de données.

46. Support d'enregistrement selon la revendication 39, dans lequel :

le programme amène l'ordinateur à fonctionner en outre comme une section de génération de clé de séquence de données (626) destinée à générer une clé de séquence de données sur la base d'une séquence de données appliquée en entrée à un dispositif de décryptage ou fournie en sortie depuis celui-ci, et

la section de génération de clé de contenu (618) génère la clé de contenu sur la base de la seconde limitation de décryptage et de la clé de séquence de données.

47. Support d'enregistrement selon la revendication 39, dans lequel :

le programme amène l'ordinateur à fonctionner en outre comme une section de génération de clé de séquence de données (626) destinée à générer une clé de séquence de données sur la base d'une séquence de données appliquée en entrée à un dispositif de décryptage ou fournie en sortie à partir de celui-ci, et

la section de génération de clé de contenu (618) génère la clé de contenu sur la base de la seconde limitation de décryptage, de la clé variable dans le temps, et de la clé de séquence de données.

FIG. 1

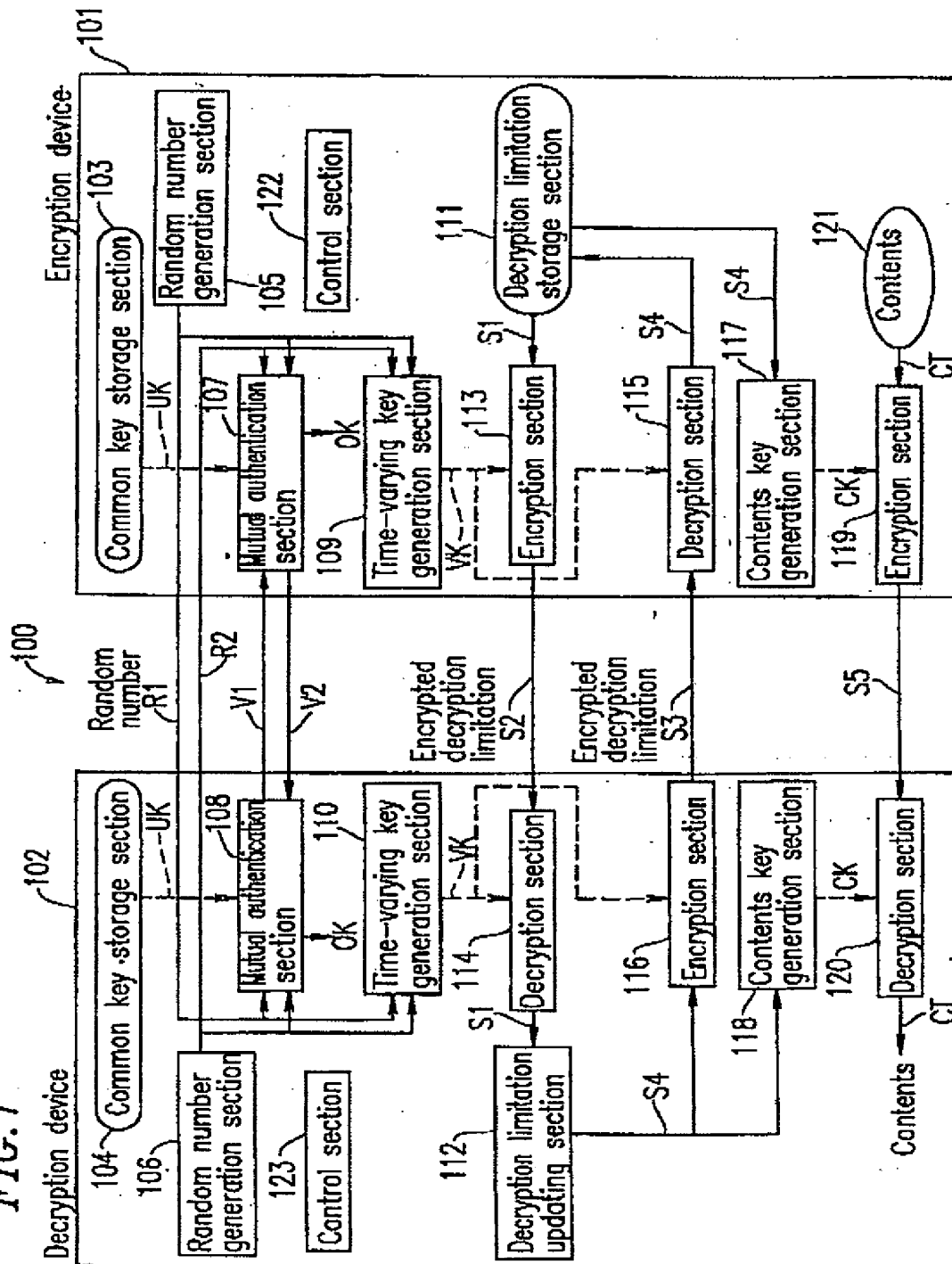




FIG. 2

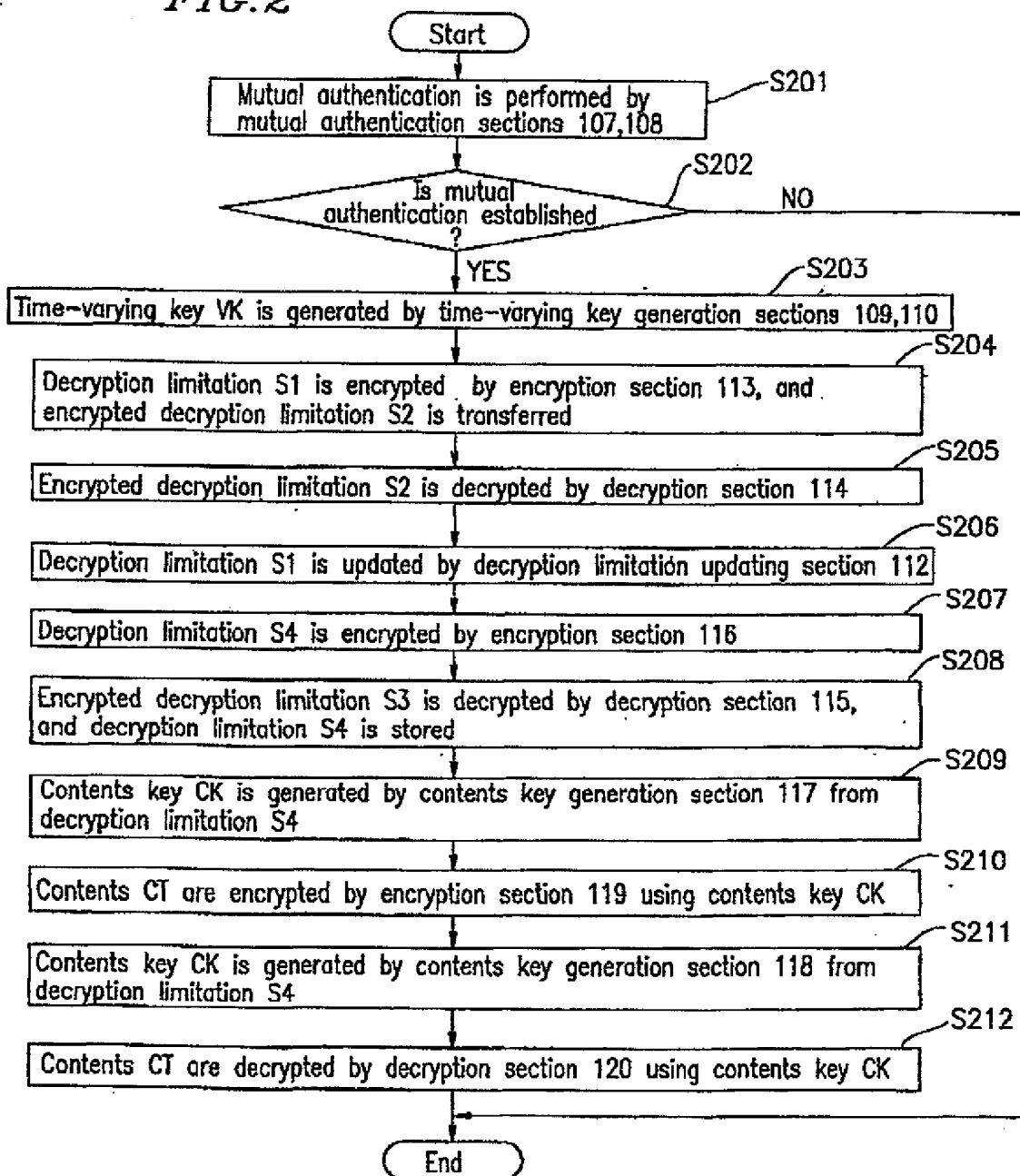


FIG. 3

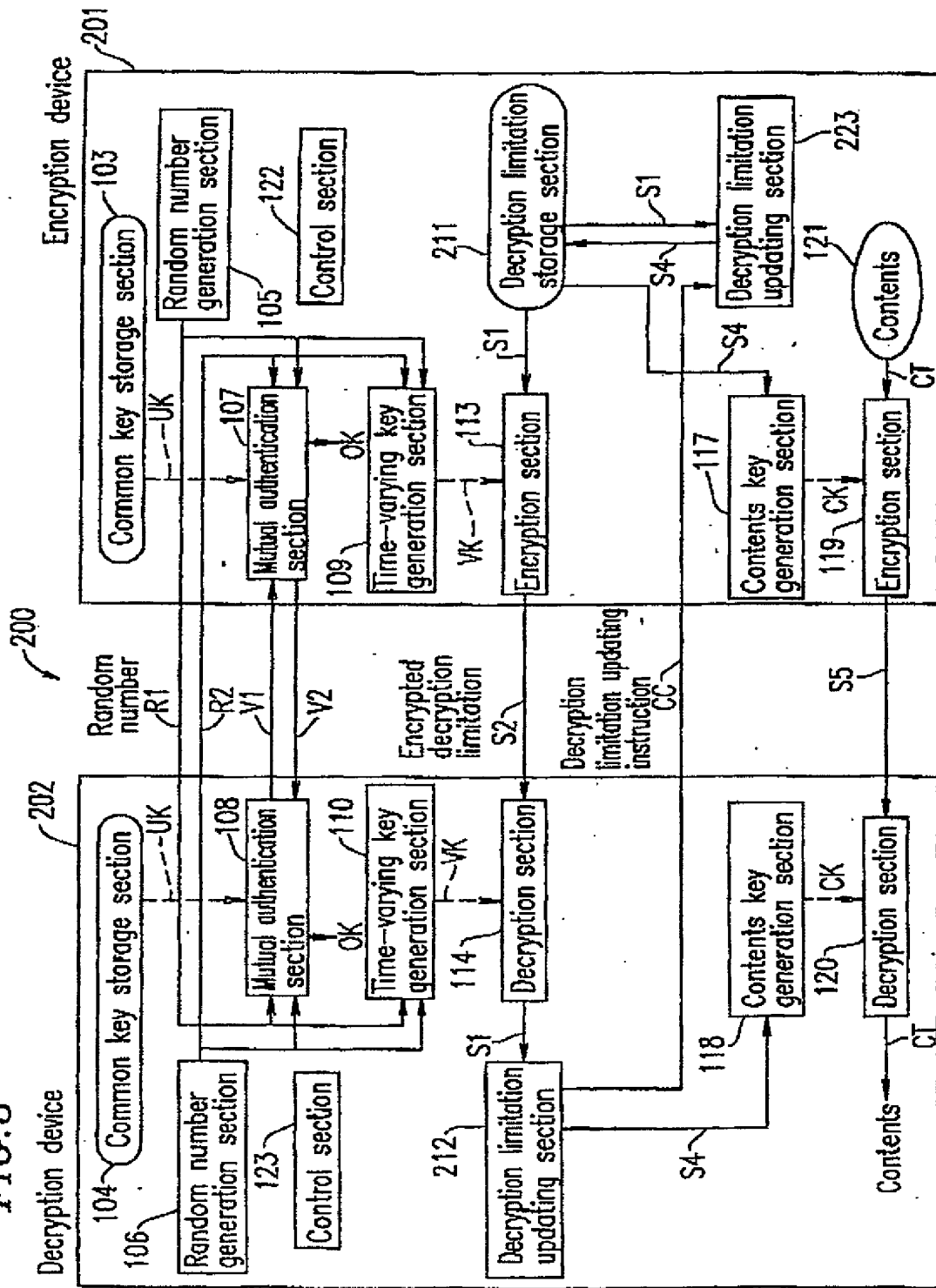


FIG. 4

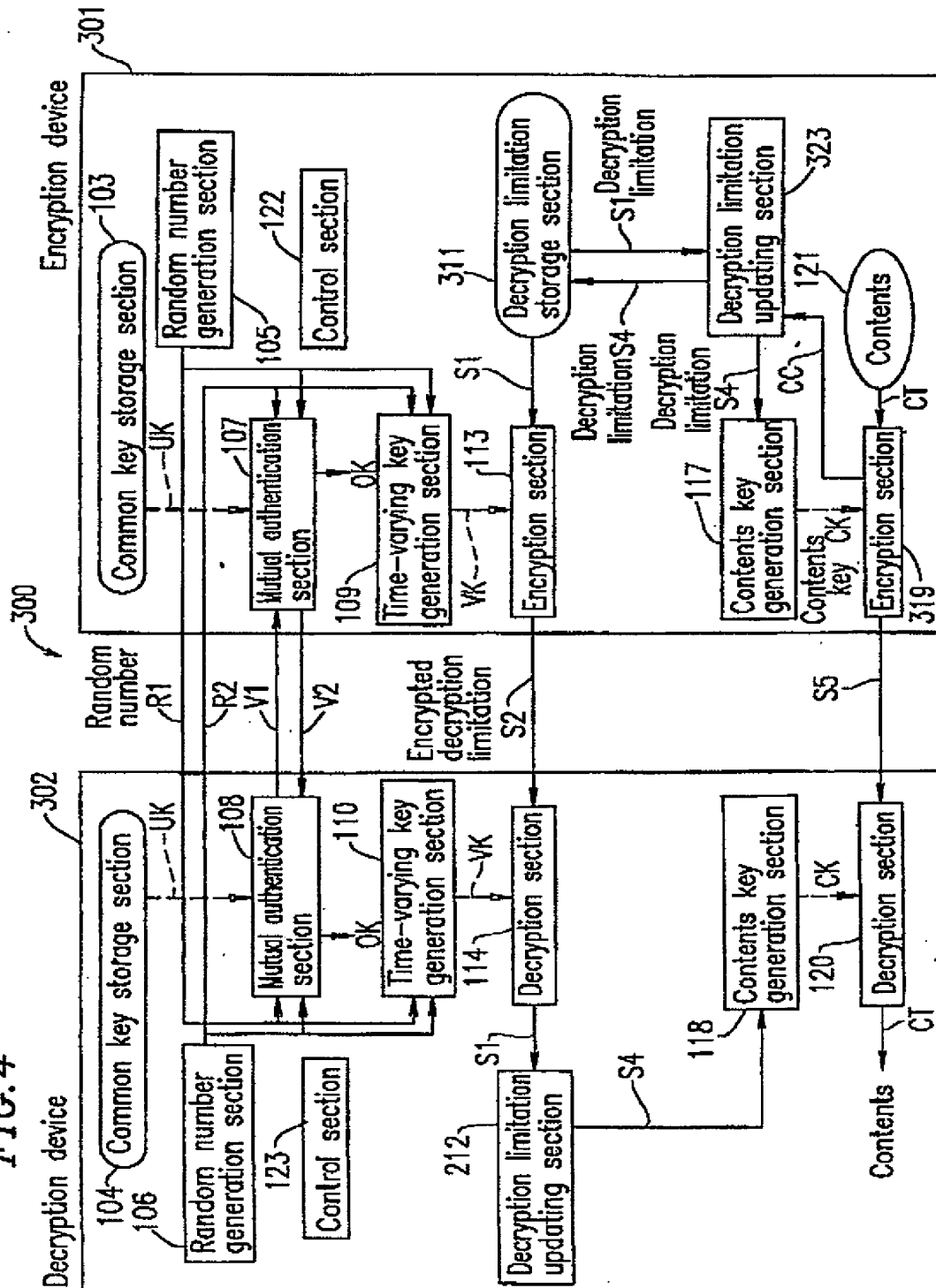


FIG. 5

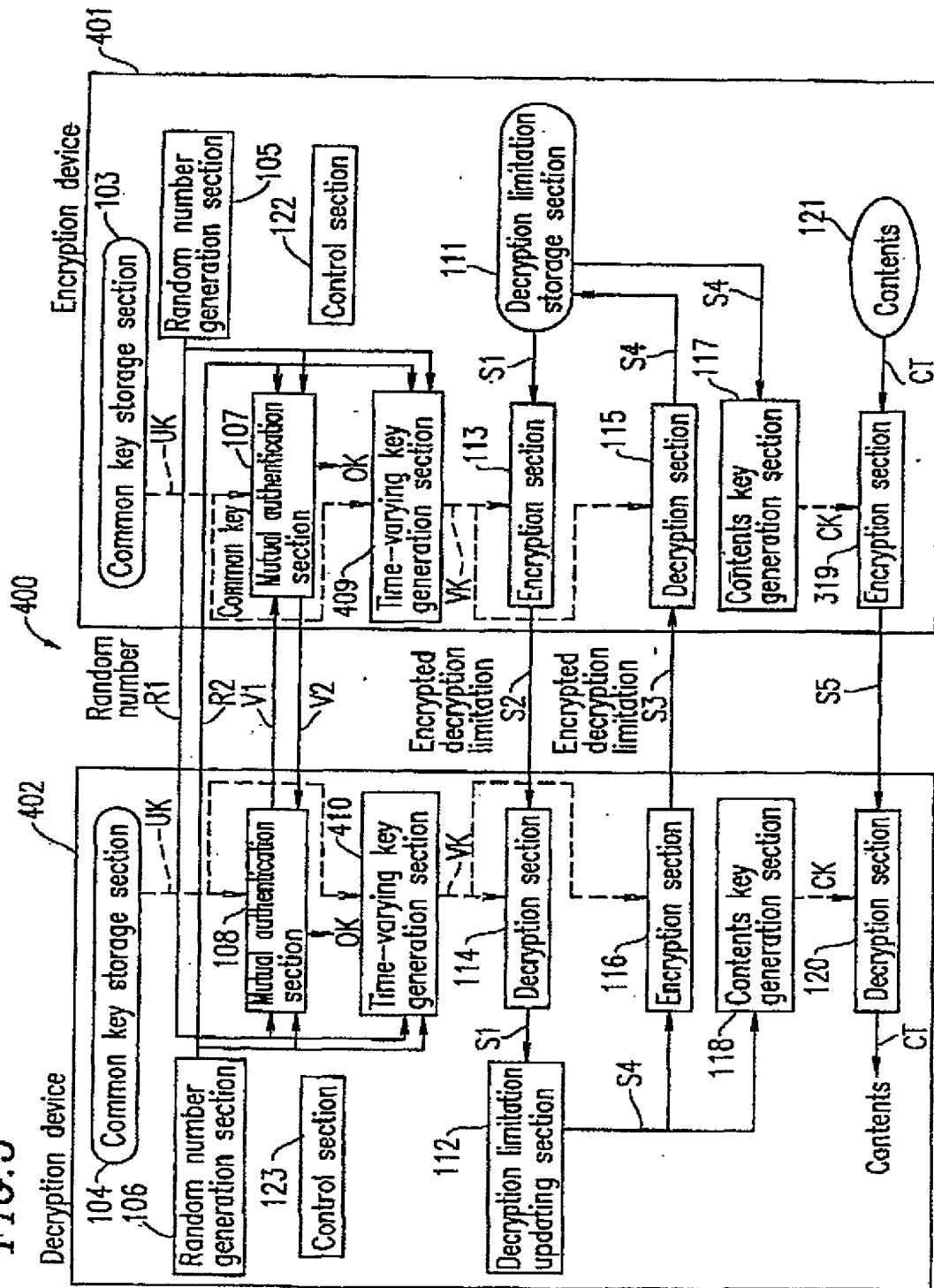


FIG. 6

